РОБОЧИЙ ЗОШИТ

ДЛЯ УЧАСНИКІВ ТРЕНІНГУ З ПИТАНЬ КІБЕРГІГІЄНИ

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні

НАДС
НАЦІОНАЛЬНЕ АГЕНТСТВО УКРАЇНИ З ПИТАНЬ ДЕРЖАВНОЇ СЛУЖБИ

USG УКРАЇНСЬКА ШКОЛА УРЯДУВАННЯ

Die Bundesregierung

UKaid from the British people

РОБОЧИЙ ЗОШИТ

ДЛЯ УЧАСНИКІВ ТРЕНІНГУ З ПИТАНЬ КІБЕРГІГІЄНИ

ЗАГАЛЬНА КОРОТКОСТРОКОВА ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

Київ • 2021

УДК 004.4.056.5(072)
М54

Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації. – Київ: ВАІТЕ, 2021. – 262 с.

Автори-упорядники теоретичних відомостей:

Барановський Олексій Миколайович, доцент кафедри інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського, національний спеціаліст проектів Координатора проектів ОБСЄ в Україні – теми: «Безпечне користування мережею «Інтернет», «Безпека користування соціальними мережами»;

Гузій Василь Володимирович, колишній Начальник відділу протидії злочинам у сфері платіжних систем Управління боротьби з кіберзлочинністю МВС України, експерт з кібербезпеки та дослідник кіберзагроз, національний спеціаліст проектів Координатора проектів ОБСЄ в Україні – теми: «Соціальна інженерія», «Шкідливе програмне забезпечення»;

Майорников Демид Ігорович, засновник та виконавчий директор компанії Sekurno, національний спеціаліст проектів Координатора проектів ОБСЄ в Україні – теми: «Безпечне користування електронною поштою», «Фізична безпека»;

Манжай Олександр Володимирович, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент, національний спеціаліст проектів Координатора проектів ОБСЄ в Україні – теми: «Вступ», «Безпека мобільних пристроїв», «Убезпечення від неправдивих повідомлень», «Правові засади кібергігієни».

Автори-упорядники практикуму:

Манжай Олександр Володимирович, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент, національний експерт з питань кібербезпеки Координатора проектів ОБСЄ в Україні – модулі: «Соціальна інженерія», «Безпечне користування мережею "Інтернет"», «Безпека мобільних пристроїв», «Убезпечення від неправдивих повідомлень», «Правові засади кібергігієни»;

Носов Віталій Вікторович, професор кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент, національний експерт з питань кібербезпеки Координатора проектів ОБСЄ в Україні – модулі: «Безпечне користування електронною поштою», «Шкідливе програмне забезпечення»; «Безпека користування соціальними мережами», «Фізична безпека».

Загальне керівництво проектом:

Ольга Войтович, національна спеціалістка проектів Координатора проектів ОБСЄ в Україні.

ISBN 978-617-7627-50-9

ЗМІСТ

ЧАСТИНА І
ТЕОРЕТИЧНІ ВІДОМОСТІ

ВСТУП

Сьогодні безпека роботи з інформацією, як ніколи, є актуальною. Зростаючі кібератаки на державні та приватні підприємства, установи й організації тільки посилюють цей тренд. Окрема категорія загроз стосується громадян, які все частіше стають об'єктом прискіпливої уваги правопорушників. Враховуючи викладене, поступово набуває поширення відносно нова концепція необхідності самостійного дотримання користувачами елементарних правил безпеки. Такий підхід дає змогу значно посилити систему колективної безпеки суспільства та держави в цілому. Агентство Європейського Союзу з мережної та інформаційної безпеки (European Union Agency for Network and Information Security) зазначає, що кібергігієна повинна розглядатися так само, як особиста гігієна, і, після належної інтеграції в організацію, має стати простою повсякденною процедурою, яка забезпечить оптимальний стан кіберздоров'я організації[1].

Порушення правил кібергігієни може призвести для згубних наслідків не лише для окремої людини. Досить часто від дій зловмисників страждає і роботодавець жертви. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники використовують окрему особу як лаз для проникнення на об'єкти критичної інфраструктури, викрадення чутливих державних даних, створення умов для скоординованих повномасштабних атак.

Таким чином, недотримання вимог кібергігієни здатне завдати значної матеріальної та моральної шкоди. А крім того, суттєво вплинути на Вашу особисту репутацію!

У світі існує достатньо велика кількість тлумачень слова «кібергігієна». Вони, як правило, відображають найбільш значущі аспекти цього терміна, важливі для конкретної галузі знань. Серед останніх оприлюднених визначень можна навести такі:

[1] Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security(ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p.4

- правила кібербезпеки, яких мають дотримуватися онлайн-користувачі з метою забезпечення цілісності та убезпечення своїх персональних даних на мережних пристроях від компрометації у випадку кібератаки[2];
- сукупність практик, спрямованих на захист від негативного впливу на певні об'єкти ризиків, пов'язаних з кібербезпекою[3];
- способи заохочення користувачів комп'ютерних технологій до безпечної поведінки в інтернеті[4].

Більш спрощена інтерпретація цього терміну дозволяє представити ***кібергігієну*** як дотримання правил безпечної поведінки у кіберсфері.

Така поведінка обумовлена наявністю загроз, які виникають під час роботи користувачів з інформацією в електронному вигляді. Спроби реалізації загроз називаються атаками.

Як і під час риболовлі або полювання, зловмисники можуть заздалегідь обирати цілі, які вважають цікавими для себе, а можуть навпаки розставити пастки і чекати, доки жертва потрапить в одну з них. Теж саме стосується ситуацій, коли порушники випадковим чином обирають жертву, стосовно якої намагаються реалізувати свої наміри.

Виділяють декілька типів *інформаційних атак*: соціальна інженерія, одержання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через ЗМІ, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів тощо[5].

Перед тим, як напасти, зловмисниками можуть здійснюватися підготовчі дії. Це виражається у підшукуванні працездатних схем нападу, збиранні інформації про жертву різними способами, створенні умов для реалізації атаки.

Для того, щоб мінімізувати ризик успішної реалізації таких атак, як раз і потрібна кібергігієна. По суті, це рутинний процес. І для того, щоб полегшити його,

[2] Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).

[3] Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).

[4] Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*. 2014. Vol. 11. Iss. 4. pp. 489-510. (DOI: 10.1515/jhsem-2014-0035).

[5] Sharma S. Gupta J. N. D. Securing Information Infrastructure from Information Warfare. *Logistics Information Management*. 2002. № 15(5/6). P. 416.

потрібно використовувати допоміжний інструментарій. Якщо у класичній гігієні такими інструментами є мило, шампунь, зубні щітка тощо, то для забезпечення її кібернетичного аналогу використовуються спеціальні програми, як от: антивіруси, фаєрволи, захищені браузери та багато інших застосунків і сервісів.

Важливим моментом у роботі з інструментами кібергігієни є правильне їх застосування. Це приблизно те саме, що і правильне підрізання нігтів ножицями або зачісування волосся гребінцем. З одного боку, все просто, а з іншого – потрібно чітко визначити для себе елементарний порядок дій з певними програмами, щоб не потрапити у халепу. Просте озброєння купою застосунків для захисту інформації, як правило, не приносить користі. Без знання правил роботи з такими програмами вони стають просто набором коду, який навряд чи зможе Вас захистити.

Так само потрібно мати на увазі, що чим меншою буде кількість інформації, яку Ви хочете вберегти, тим менше Вам потрібно буде вживати дій для її убезпечення. Тому під час продукування фотознімків, написання повідомлень в мережі, спілкування телефоном з незнайомими та навіть знайомими людьми подумайте, чи дійсно це є необхідним і наскільки шкідливим може бути використання відповідної інформації проти Вас.

Саме тому бажано користуватися перевагами інтернету щодо забезпечення анонімності та використання вигаданих даних. Особливо це стосується мережних ресурсів, у безпеці яких не можна бути впевненим. У випадку атаки на Вас, зловмисники зможуть отримати доступ лише до вигаданих даних. Це може стати ще одним додатковим ешелоном, який убезпечить Вас від протиправних посягань.

Немаловажним принципом забезпечення кібергігієни є періодичне резервування даних. Можна використовувати мережне резервування або дублювання даних на фізичних запам'ятовувальних пристроях. Усе залежить від чутливості даних, які потрібно зберегти, та відповідних знань предметної області. Так, наприклад, другорядні дані цілком можуть бути перенесені у хмару. Це дозволить зменшити кількість інформації, що потребує захисту на локальних пристроях, і таким чином тримати їх у чистоті.

Найкращий варіант, якщо Ви зробите кібергігєну своєю повсякденною звичкою. При цьому вона не потребує суттєвих витрат коштів і часу. Згодом Ви звикнете до виконання відповідних процедур і відчуєте їх корисність як в особистих, так і в службових справах.

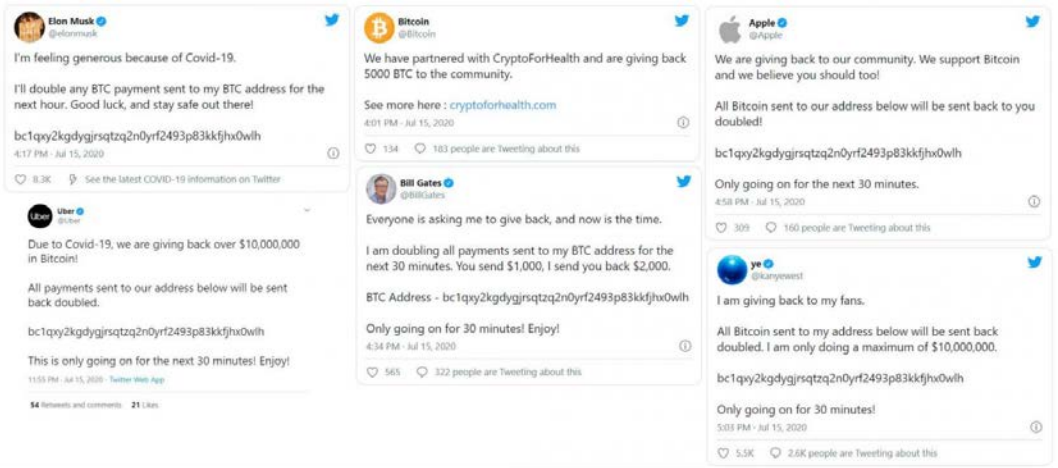
Пам'ятайте: дотримуватися правил кібергігієни – це не тільки корисно, але й розумно і комфортно!

МОДУЛЬ № 1:

СОЦІАЛЬНА ІНЖЕНЕРІЯ

«ХАКЕРИ ЗЛАМАЛИ СОЦІАЛЬНУ МЕРЕЖУ "ТВІТЕР" ЗА 24 ГОДИНИ»

У середині липня 2020 року мережу «Інтернет» сколихнула новина, що хакери зламали соціальну мережу «Твітер», отримали доступ до акаунтів відомих політиків, бізнесменів, акторів та компаній, у тому числі: Барака Обами, Елона Маска, Джефф Безос, Uber, Apple тощо, – та від їх імені розмістили неправдиві повідомлення, що біткоїни, надіслані на гаманці, вказані у твітах протягом 30 хв будуть повернуті у подвійному розмірі:



Це тардійний прийом соціальної інженерії – видати себе за представника офіційної організації, банку чи державної структури та змусити жертву переказати кошти, повідомити свої персональні дані чи вчинити інші компрометуючі дії, які особа за жодних обставин не вчинила б, якби не була обманутою.

За такої схеми злочинцям вдалося зібрати близько 13 біткоїнів, що по курсу становило близько USD 118,000.

У ході атаки хакери отримали доступ до 130 твітер-акаунтів, 45 з них вдалось одразу заблокувати та змінити паролі доступу. Персональні дані користувачів окремих акаунтів були викрадені.

Під час розслідування стало відомо, що хакери отримали доступ до акаунтів користувачів твітеру через панель управління, яка використовувалася співробітниками «Твітеру» для модерування соціальної мережі. Однак найцікавішим є те, що хакери отримали доступ до панелі управління не через вірусну атаку чи використання вразливості програмного забезпечення, а шляхом типової фішингової атаки із використанням методів соціальної інженерії. Хакери зателефонували співробітникам «Твітеру» та обманом отримали від них дані для доступу до панелі управління соціальної мережі та в подальшому викрали паролі від акаунтів користувачів.

Атакуючими виявилися 17-річний мешканець Флориди Грем Айвен Кларк (Graham Ivan Clark), 19-річний британець Мейсон Джон Шепперд (Mason John Sheppard), та 22-річний американець Німа Фазели (Nima Fazeli).

Вдала атака 2020 року на «Твітер», одну із топових світових компаній, із використанням **виключно методів соціальної інженерії,** безумовно, є безпрецедентним випадком та буде використовуватися як "case study" у підручниках із соціальної інженерії.

Цей інцидент засвідчує, що, не зважаючи на мільярдні витрати компаній та урядів на кібербезпеку, програмне забезпечення, антивірусні програми та фаєрволи, хакери можуть потрапити у вашу компанію через відкриті навстіж двері "чорного ходу."

1. ПОНЯТТЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія (далі по тексту СІ) у більш широкому розумінні – це наука, що вивчає людську поведінку та фактори, які на неї впливають.

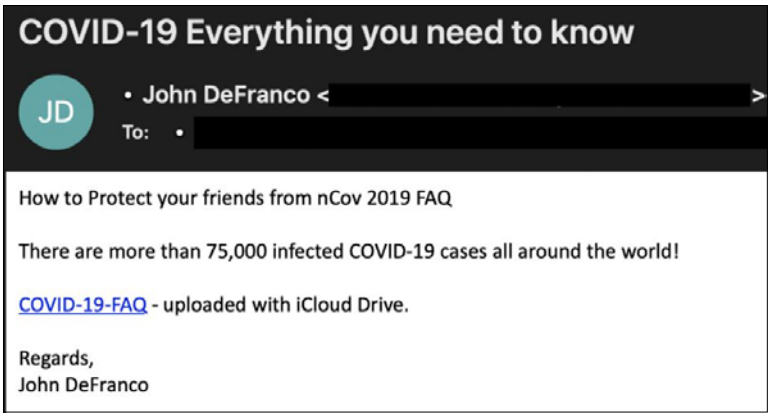
Основною метою соціальної інженерії є дослідження причин тієї чи іншої поведінки людини; а також обставин та середовища, що впливають на формування системи цінностей індивіду, і як наслідок – їхньої поведінки.

У контексті інформаційної безпеки, СІ – це психологічне маніпулювання людьми, щоб змусити їх вчинити певні дії, наприклад повідомити свої персональні дані,

перейти та завантажити файл за посиланням тощо, які особа не вчинила б, якщо б нею не маніпулювали.

▶ *Які зовнішні фактори хакери можуть використовувати на свою користь для планування та здійснення атак із використанням методів соціальної інженерії?*

- Епідемії, поширення хвороб, стихійні лиха. Прикладом може бути пандемія COVID-19. На малюнку нижче Ви бачите приклад фішингового листа, який як приманку використовує страх пандемії COVID-19, та схиляє користувача завантажити нібито інформаційний бюлетень, як захистити себе та рідних від зараження. Насправді у додатку до листа знаходиться вірус.

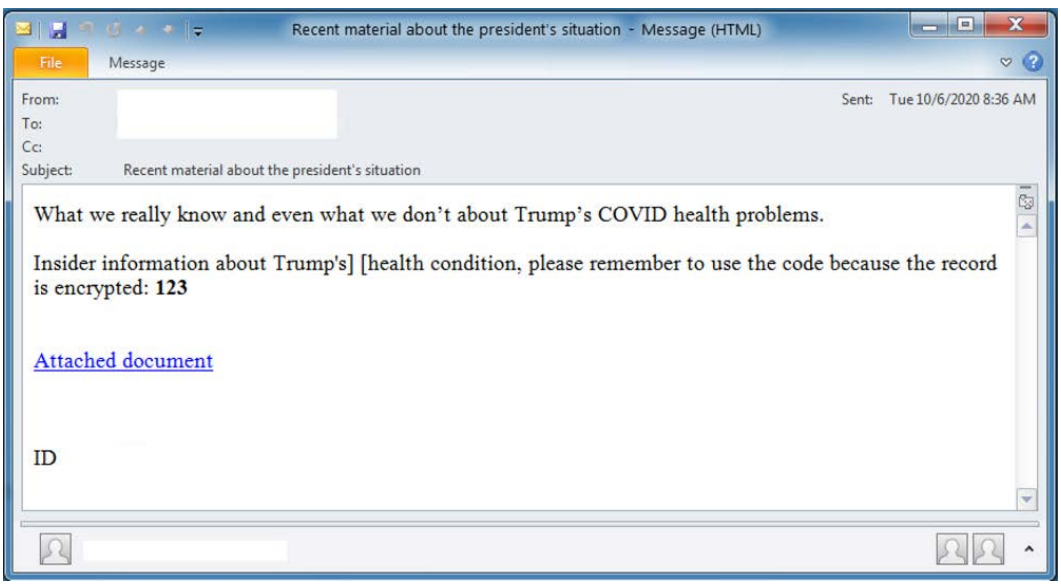


У квітні 2020 року, Український CERT (The Community Emergency Response Team – спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України) повідомляв про фішингові кампанії із використанням епідеміологічної ситуації у світі. Згідно з повідомленням на офіційному сайті Центру, зловмисники надсилали користувачам листи з нібито офіційних поштових скриньок (наприклад, moz_ukraine@i.ua) та прикріплювали інфіковані файли, які містили у собі атрибути офіційних документів Міністерства охорони здоров'я – бланки, та мають розширення .doc, .docx, .xls, .xlsx, .ppt, .pptx тощо. Інфікування пристроїв користувачів відбувається у момент відкриття такого файлу (https://cert.gov.ua/article/26).

Ще один приклад фішингової атаки із використанням пандемії COVID-19, як важеля впливу на жертву, наведено на малюнку, що нижче. Хакери надсилали нібито мапу розповсюдження COVID-19, яка була у формі Java-архіву і коли користувач його завантажував, на його комп'ютер потрапляв вірус, найчастіше це був вірус типу «викрадач інформації».

- Економічні катаклізми та події у світі. На малюнку, що нижче, Ви бачите СМС-повідомлення про нібито зарахування коштів на рахунок в рамках допомоги із державного фонду Канади. Повідомлення містить посилання на фішинговий сайт.

- Політичні події, вибори, політичні персоналії. Перед виборами в США у 2020 році та з новин напередодні стала розповсюджуватися інформація, що у чинного президента Дональда Трампа діагностували коронавірус. Фахівці із кібербезпеки почали фіксувати фішингові кампанії, які намагалися використати цю новину для розповсюдження троянських програм. Користувачам мережі на електронну адресу надходили листи, що це повідомлення містить інформацію щодо стану здоров'я Дональда Трампа, та для отримання більш детальних даних пропонувалося перейти за посиланням. Коли користувачі переходили за посилання, на їх комп'ютер завантажувався вірус.



Ще один приклад стосується фішингових атак на українські державні структури, де як приманку використовували електронні листи із вкладеним нібито документом щодо ситуації на лінії зіткнення в Донецькій та Луганській областях. Документ містив шкідливий макрос, який завантажував троянську програму.

Міністерство закордонних справ України
Михайлівська площа 1, м. Київ, 01018
e-mail: zsmfa@mfa.gov.ua

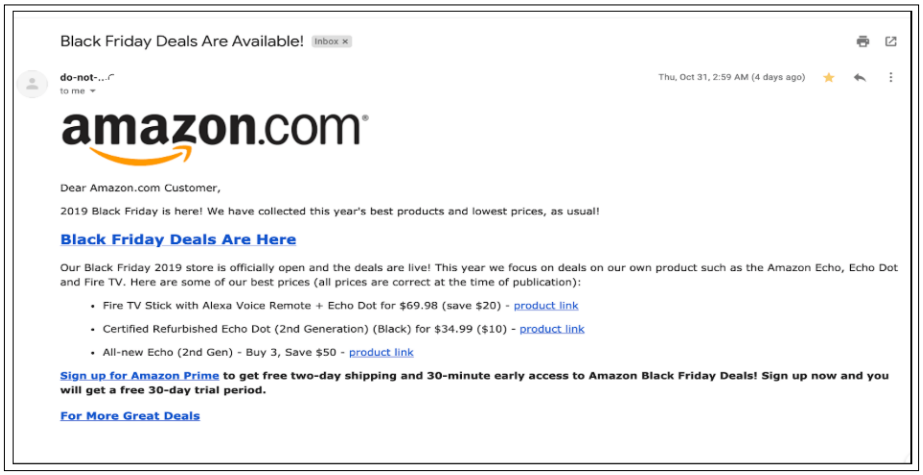
КОПІЯ:
ГУР МОУ

Українська сторона СЦКК повідомляє, що не дивлячись на прийняті домовленості про повний та безстроковий режим припинення вогню, який вступив в дію з 27 липня 2020 року, російськими окупантами були порушені взяті на себе домовленості та 29.07.2020 року, з непідконтрольного урядові України території поблизу селища Доломітне був здійснений провокаційний обстріл в напрямку селища Новолуганськ. Ворог застосував гранатомет ГП-25 здійснивши один постріл по позиціям наших захисників.

Підрозділи ЗС України не порушуючи свою бойову готовність, вогонь у відповідь не відкривали та по цей час дотримуються взятих на себе домовленостей, щодо цілковитого припинення вогню.

В свою чергу представники УС СЦКК оперативно звернувшись до чергового СММ ОБСЄ, засвідчили дані порушення та вимагали негайного впливу на представників російсько-окупаційних військ, щодо припинення обстрілу та дотримання гарантій безпеки ворогом.

- Свята, знаменні події, ярмарки, концерти тощо. Напередодні великих та загальнонаціональних свят, як правило, фіксують збільшення шахрайських атак. Так, на малюнку нижче зображено лист, нібито від онлайн магазину “Amazon” щодо знижок до «Чорної п’ятниці». Насправді, це фішинговий лист, який має на меті викрадення персональних даних.



https://us-cert.cisa.gov/ncas/tips/ST04-014

Чому хакери використовують СІ?

- По-перше, це дешево і СІ не вимагає таких значних затрат, як на розробку ШПЗ чи експлойтів;
- По-друге, це ефективно. СІ до сьогодні вважається одним із найефективніших методів хакерських атак. Атаки із використанням СІ є передумовою та відправною точкою атак із використанням ШПЗ. Хакери застосовують СІ для отримання первинного доступ до мережі, а вже потім застосовують складне ШПЗ, щоб надійно «засісти» в системі, викрасти дані тощо. Розробити ШПЗ чи знайти вразливість у програмному забезпеченні – це тільки частина атаки, важливо «переконати» жертву перейти за посиланням та завантажити ШПЗ;
- По-третє, СІ ефективна проти будь-якої операційної системи та версії програмного забезпечення, від неї не захистять антивіруси.

2. МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Традиційно виділяють такі методи СІ (зверніть увагу, що цей перелік може відрізнятися, залежно від джерела вивчення чи експертної думки):

«Фішинг» – це один із найрозповсюдженіших прийомів СІ. Під час фішингової атаки зловмисник під виглядом іншої особи, організації, відомого сервісу тощо, намагається отримати від потерпілого його персональні дані чи іншу конфіденційну інформацію або змусити вчинити дії, які особа не вчинила б за звичайних умов, наприклад, завантажити та встановити шкідливе програмне забезпечення. Традиційним видом фішингу є електронний лист від банку із повідомленням, що, у зв'язку із технічними неполадками або загрозою хакерської атаки «банк» проводить планову зміну паролей усіх користувачів та просить користувача ввести свій старий пароль для верифікації. Іншим прикладом фішингу, може бути точна копія вебсайту інтернет-магазину, де користувачеві пропонують ввести дані платіжної картки. Звичайно, що після їх введення кошти з картки зникають.

Перед здійсненням фішингової атаки шахрай створює точну копію сайту компанії чи організації, «від імені» якої буде надсилати листи. Якщо йдеться про електронний лист, то атакуючий копіює форму, шрифти та елементи офіційних листів від банку та відтворює їх у повідомленні.

Різновидом фішингу є цільовий або таргетований фішинг, який націлений на конкретну особу або користувача. Це є складнішою атакою, оскільки передбачає досконале вивчення цілі перед атакою, її звичок, історії, взаємовідносин у колективі, з рідними чи керівництвом.

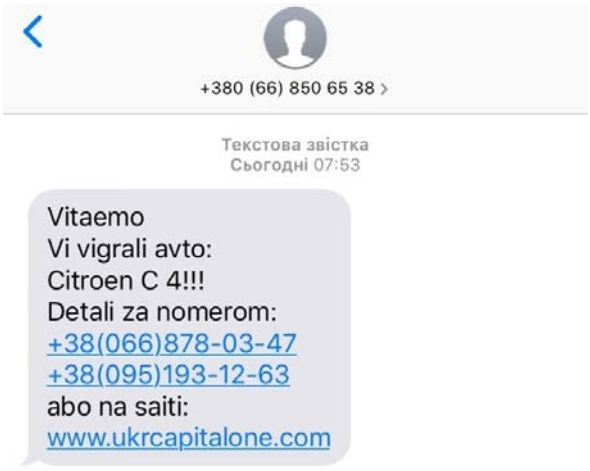
Наприклад, шахрай знає, що керівник установи зупинявся в готелі «Львів», таким чином він надсилає електронний лист нібито від адміністрації готелю із додатковим рахунком за користуванням баром. Керівник відкриває файл та завантажує вірус на свій комп'ютер.

«Вішинг» – це різновид фішингу, який здійснюється через телефон. Яскравими прикладом вішингу є дзвінок нібито із банку, де атакуючий повідомляє, що він співробітник банку та під вигаданим приводом просить особу повідомити дані своєї платіжної карти. Зазвичай зловмисник повідомляє про блокування картки, іноді шахраї говорять, що службою безпеки банку нібито проводиться звіряння особистих даних клієнтів, щоб убезпечити їх від шахрайства.

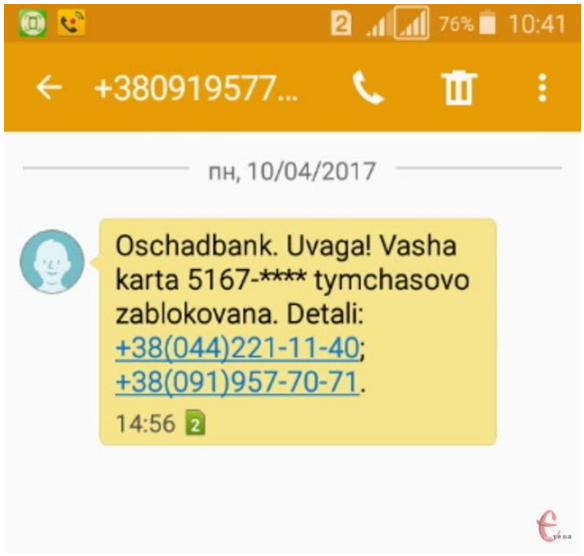
Іншим прикладом є шахрайство типу «Ваш родич потрапив в аварію чи до поліції». Найчастіше шахраї здійснюють такого роду дзвінки вночі або рано-вранці, коли людина сонна, погано міркує. Шахраї, як правило, розмовляють чітко, впевнено та помірно швидко, щоб не дати змоги жертві зважити ситуацію та поміркувати. Під час дзвінків «із поліції» шахраї роблять ставку на розгубленість жертви та застосовують методи психологічного тиску, змушуючи особу «вирішувати справу зараз і тепер, бо немає часу зволікати».

«Вішинг» є одним із найстаріших видів шахрайства, однак із розвитком комп'ютерних технологій «вішинг» отримав нові можливості. IP-телефонія та комп'ютерні технології дозволяють легко змінити номер телефону чи наприклад голос телефонуючого, в ході розмови можна включати технічні записи, наприклад, автовідповідач банку тощо.

«SMS-фішинг» – це різновид фішингу, який здійснюється через СМС-розсилки. Одним із яскравих прикладів є СМС-повідомлення нібито про виграш великої суми грошей або автомобіля. Однак, щоб отримати виграш, необхідно внести 10% за «оформлення» необхідної документації тощо.



Яскравим прикладом СМС-шахрайства є повідомлення від банків:



«Кві про кво» (від лат. Quid pro quo) – цей метод соціальної інженерії поєднує в собі ознаки фішингу та вішингу. Як правило, шахрай телефонує співробітникові

компанії, найчастіше із підміною номеру, щоб він виглядав як корпоративний, та представляється службою технічної підтримки. Шахрай повідомляє, що виникли певні технічні проблеми і, щоб їх усунути, потрібно, щоб співробітник вчинив певні дії. Як правило, під «керівництвом» несправжнього представника служби технічної підтримки нічого не підозрюючий співробітник встановлює в себе ШПЗ або надає атакуючому віддалений доступ до комп'ютера.

«Дорожнє яблуко» («road apple») або «Троянський кінь» – це метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний носій інформації (флеш-накопичувач, диск) із шкідливим програмним забезпеченням. Носій може мати логотип компанії чи напис, що зацікавить співробітника, наприклад «список на звільнення», «заробітна плата за жовтень» тощо. Як тільки співробітник вставить такий носій до комп'ютеру, запуститься шкідливий код, який активує бекдор та надасть атакуючому доступ до мережі.

«Зворотна соціальна інженерія» – це вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані. Одним із можливих сценаріїв є, коли шахрай надсилає співробітникам компанії нібито нові номери телефонів служби технічної підтримки. Цілком імовірно, що через деякий час хтось із співробітників зателефонує і шахрай зможе вивідати інформацію, яка його цікавить.

Складна атака через проміжну ціль ("Supply chain attack"). У більш широкому розумінні поняття "supply chain attack" використовується для опису складної, декілька ступеневої атаки, під час якої хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компрометує ту ціль, яка від самого початку його цікавила. "Supply chain" атаки характерні для промислового, фінансового сектору та державних установ. До прикладу, хакер обрав своєю ціллю банк, однак після вивчення цілі зрозумів, що установа має високий рівень захисту і просто так її не скомпрометувати. В такому випадку хакер може сфокусуватися на атаці підрядників банку, скажімо невеликої компанії, яка розробляє чи обслуговує сайт чи бази даних банку, або, наприклад, підрядника, який обслуговує банкомати. Невеликі компанії, як правило, менш захищені, а тому успішно скомпрометувати їх набагато простіше. Скомпрометувавши, скажімо, розробника вебсайтів, хакер зможе інтегрувати шкідливий програмний

код в програмне забезпечення підрядника, яке у подальшому буде встановлене на системах банку, і хакер таким чином отримує несанкціонований доступ до самого банку.

Яскравим прикладом "supply chain"-атаки була масштабна хакерська атака 2017 року з використанням різновиду вірусу Petya, що спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, «Укртелеком», «Укрпошта», «Ощадбанк», «Укрзалізниця» та низки інших великих підприємств. Ця атака розпочалася із компрометації системи оновлення програми M.E.Doc. Інфіковані файли з оновленнями M.E.Doc були встановленні на тисячі систем та спричинили блискавичне розповсюдження вірусу Petya.

У контексті соціальної інженерії "supply chain"-атаки працюють за таким же принципом. Якщо кінцевою ціллю хакера є установа або урядовець, системи яких надійно захищені, хакер може сфокусуватися на компрометації їх близьких, родичів, підлеглих або підприємств, які обслуговують головну ціль.

Як приклад можна навести фішингову атаку на фінансового спеціаліста одного із великих банків Європи. Хакери спочатку провели фішингову кампанію щодо працівників банку, розіславши спам на їхні службові адреси електронної пошти, однак спрацювали спам фільтри та внутрішні системи захисту – атака виявилась невдалою. Тоді хакери розіслали таргетовані фішингові листи усім ТОП-менеджерам банку. Один із фінансових спеціалістів, використовував свій персональний комп'ютер у службових цілях і не мав там належного захисту. Таким чином, відкривши листа він запустив вірус та хакери отримати реквізити доступу до внутрішньої мережі банку.

Тактику "supply chain"-атаки обрала у 2017 році хакерська група Cobalt, внаслідок чого провела десятки вдалих атак на фінансові установи країн СНД.

Висновок: пам'ятайте, справжньою ціллю хакера можете бути не Ви, а Ваш керівник чи установа, де Ви працюєте, а Ви – це лише інструмент у досягненні цілі.

Намагайтеся мінімізувати використання домашнього комп'ютера у службових цілях. Якщо все ж таки це необхідно, переконайтесь, що Ви користуєтесь програмним забезпеченням останніх версій, у Вас встановлено антивірус, firewall тощо.

▶ *Які психологічні прийоми використовують шахраї для впливу на жертву?*

У своїй книжці «Психологія впливу» професор психології Роберт Чалдіні виділив шість принципів або рушіїв впливу на людей:

- *Взаємність* – людина намагається відповісти добром на добро, послугою на послугу, щоб сплатити свій «борг». Почувати себе «зобов'язаним» комусь не комфортно, тому ми намагаємось якнайшвидше позбутися цього обов'язку. Якщо Ваш колега зробив Вам послугу або Ваш друг запросив Вас на вечірку, Ви відчуваєте внутрішній обов'язок відповісти послугою на послугу, запросити друга на вечірку також. Яскравим прикладом використання принципу *взаємності* є поведінка офіціантів у ресторанах. Перед тим, як принести Вам рахунок, офіціант зробить Вам невеликий «подарунок», це може бути жуйка чи цукерка, наприклад. У такій ситуації Ви відчуваєте себе зобов'язаним «відплатити» офіціанту щедрими «чайовими». Сценаріїв атак із використанням цього прийому СІ безліч. Наприклад, вступаючи у листування із жертвою, хакер може поділитися нібито якоюсь конфіденційною інформацією про свою компанію і тим самим спровокувати жертву розкрити деталі про свою установу. Хакер може запропонувати свої послуги із налаштування обладнання, надання консультації тощо, а потім попросити про взаємну послугу.

Будьте уважні, коли маловідомі Вам люди, повідомляють Вам дані або пропонують послуги, про які Ви не просили.

- *Послідовність* — людині властиво дотримуватися тих дій або вчинків, які вона вже робила у минулому. Коли людина дає обіцянку, то вважає за свій обов'язок зробити все, щоб її дотримуватися. Варто попросити людину про кілька дрібних послуг, які вона зазвичай виконує, а у потрібний момент попросити про «головну» послугу і людині буде вже незручно відмовити. Хакер може спочатку спровокувати жертву розкрити малий обсяг інформації та, користуючись принципом *«послідовності»*, досягти своєї мети та отримати дані, за якими він полював. Наприклад, якщо у

Вас одразу запитають пароль доступу до внутрішньої WiFi-мережі, Ви найімовірніше відмовите, однак якщо хакер спочатку попросить пароль до мережі WiFi, виділеної для відвідувачів закладу, а потім скаже, що не може приєднатися через технічні проблеми, ймовірність того, що Ви запропонуєте пароль до внутрішньої WiFi-мережі значно зростає.

- *Соціальний конформізм:* людина погоджується з тим, що робить більшість. Особливо в ситуаціях, коли людина не впевнена, що робити, вона швидше зробить те, що робить більшість.
- *Авторитет:* людині притаманно слідувати за тими, кому вона довіряє, кого знає, хто для неї є авторитетом. Хакери користуються цим принципом, коли телефонують, представляючись співробітниками правоохоронних органів, працівниками банку; коли надсилають фішингові листи від імені керівників компаній чи відомих брендів. Саме на авторитет відомих людей розраховували хакери, коли розмістили твіти від імені Ілона Маска, Барака Обами із закликами переказати біткоїни.
- *Симпатія:* людина охочіше та швидше виконує прохання тих, хто їй симпатичний, або зробить те, що їй подобається. Використовуючи цей принцип, хакер може розпочати процес «вербування» жертви із зробленого компліменту, до прикладу, щодо фотографій із відпустки, нової зачіски чи взуття. Хакери також можуть створювати «фейкові» акаунти в соціальних мережах, використовувати модельні фотографії протилежної статі тощо.
- *Дефіцит:* людина завжди більше бажає того, що їй недоступно. Коли речі стають менш доступними, вони здаються нам більш бажаними. Якщо у нас є вибір отримати це зараз або, можливо, отримати в майбутньому, ми обираємо зараз. Цей принцип активно застосовують маркетологи у продажах. Наприклад, акції типу «тільки сьогодні і тільки – 50% знижка» зазвичай спричиняє зростання продажу. Хакери також можуть використовувати цей підхід у своїх атаках. Наприклад, створивши відчуття, що документ, файл тощо може стати скоро недоступним, хакер може значно підвищити ймовірність того, що користувач завантажить його. Інші психологічні прийоми, які використовують шахраї включають:

- штучне створення ситуації, коли рішення треба приймати «сьогодні і зараз» (різновид вищезгаданого прийому *«дефіциту»*). Людині не дають можливості подумати, прийти до тями, порадитися, тверезо зважити ситуацію. Саме на створення штучного відчуття «дефіцит часу» на прийняття рішення покладаються шахраї у схемах «Ваш родич потрапив до поліції».

- маніпулювання прагненням отримати «швидкі гроші». Сюди відносять різноманітні лотереї та вікторини. Повідомлення про виграш автомобіля, для оформлення якого необхідно нібито внести якийсь відсоток на рахунок організації, яка проводила лотерею. Різновидом маніпулювання із використанням цього прийому є такий вид шахрайства, як «Нігерійські листи». З'явився він у другій половині 90-х років XX століття, але й досі популярний, коли людям приходять подібні листи з багатьох африканських країн (Нігерії, Беніну, Того, ПАР).

Сюжети шахрайства досить різноманітні. Найчастіше листи відправляються від імені колишнього короля, президента, високопоставленого чиновника або мільйонера з проханням про допомогу в банківських операціях, пов'язаних з переведенням грошей з Нігерії або іншої країни за кордон, отриманням спадщини і т. п., нібито оподатковуваних великим податком або ускладнених внаслідок переслідувань в рідній країні.

Інший поширений варіант – листи, нібито, від працівника банку або від чиновника, який довідався про нещодавню смерть дуже багатої людини «з таким самим прізвищем», як в одержувача листа, з пропозицією надати допомогу в отриманні грошей з банківського рахунку цієї людини. Мова в листах зазвичай іде про суми в мільйони доларів і одержувачу обіцяють чималий відсоток від сум – іноді до 40%. Якщо одержувач листа відповідає шахраям, йому надсилають декілька документів. При цьому використовуються справжні печатки та бланки великих фірм і урядових організацій.

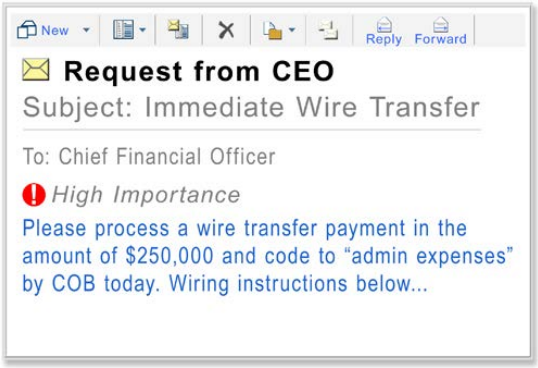
(https://uk.wikipedia.org/wiki/Нігерійські_листи)

- видавання себе за когось іншого. Сюди поряд із класичними схемами, згаданими вище, де шахрай представляється працівником банку, правоохоронного органу чи керівником організації, де працює потерпілий, можна віднести шахрайство із використанням соціальних мереж та сайтів знайомств. Шахрай реєструє акаунт від імені дівчини та втирається у довіру до жертви, а потім просить або про переказ коштів, або здійснити інші дії у своїх інтересах.

Цей метод соціальної інженерії застосовують у такому виді шахрайства, як "Business Email Compromise" (BEC). Ці атаки проводять щодо співробітників комерційних організацій, державних установ та громадських організацій, фондів тощо. Здебільшого фішингові листи адресуються працівникам фінансових департаментів, управлінь, бухгалтерії тощо. Є декілька сценаріїв. За одним із них електронний лист надходить підлеглому нібито від керівника цієї ж установи, департаменту чи відділу та містить у собі наказ, прохання щодо переказу значної суми грошей на рахунок іншої організації із зазначенням реквізитів банківського рахунку. Насправді це рахунок злочинців.

За іншим сценарієм, на адресу бухгалтерії надходить електронний лист від партнерів, клієнтів, донорів, підрядників, контрагентів із повідомленням нібито про зміну реквізитів банківського рахунку. Якщо співробітник установи не перевірить, чи дійсно підрядник, партнер змінив банківський рахунок, кошти будуть надіслані на рахунок шахрая.

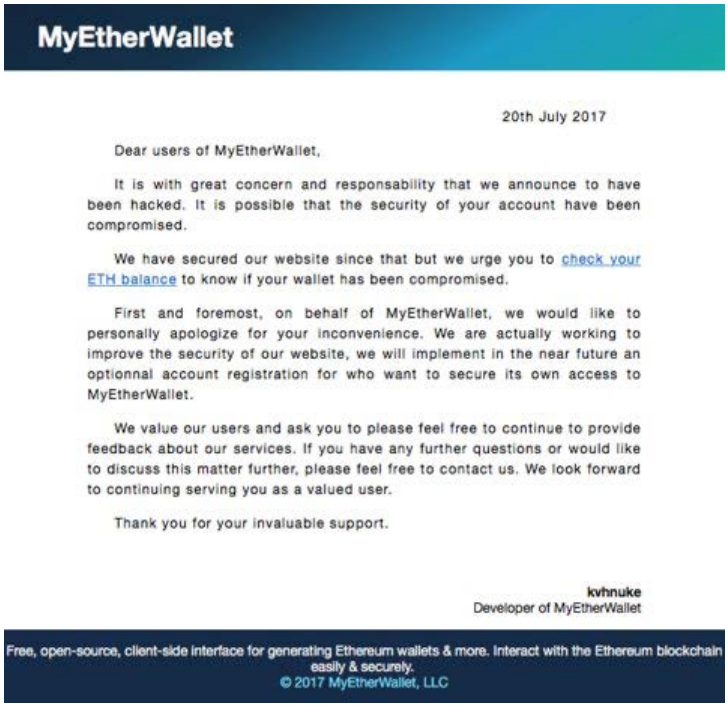
Злочинці, як правило, детально вивчають жертву та її контрагентів, і якщо їм стане відомо про угоду, що готується, то вони надішлють лист за декілька годин до підписання угоди або оплати рахунків.



- маніпулювання благими намірами потерпілого. Сюди, наприклад, входять шахрайські схеми із пожертвування грошей потерпілим від стихійного лиха, переселенцям, хворим тощо.

- маніпулювання почуттям страху. Шахраї створюють ситуацію, щоб викликати у жертви почуття страху, наприклад, втратити роботу, отримати дисциплінарне стягнення тощо. Шахраї можуть надіслати емейл із вкладеним документом «Висновок щодо результатів розгляду скарги на Іванова І.І.docx» і це буде документ із шкідливим макросом, який після відкриття завантажить на робочий комп'ютер вірус.

Іншим видом маніпулювання потерпілим є викликання у нього почуття страху за втрачені кошти. На малюнку нижче зображено фішинговий лист користувачам криптовалюти **Етеріум** про нібито хакерську атаку на компанію. Шахраї пропонували користувачу за вставленим в лист посиланням перевірити баланс на рахунку. Посилання, очевидно, було шкідливим та призводило до викрадення персональних даних.



MyEtherWallet

20th July 2017

Dear users of MyEtherWallet,

It is with great concern and responsability that we announce to have been hacked. It is possible that the security of your account have been compromised.

We have secured our website since that but we urge you to check your ETH balance to know if your wallet has been compromised.

First and foremost, on behalf of MyEtherWallet, we would like to personally apologize for your inconvenience. We are actually working to improve the security of our website, we will implement in the near future an optionnal account registration for who want to secure its own access to MyEtherWallet.

We value our users and ask you to please feel free to continue to provide feedback about our services. If you have any further questions or would like to discuss this matter further, please feel free to contact us. We look forward to continuing serving you as a valued user.

Thank you for your invaluable support.

kvhnuke
Developer of MyEtherWallet

Free, open-source, client-side interface for generating Ethereum wallets & more. Interact with the Ethereum blockchain easily & securely.
© 2017 MyEtherWallet, LLC

- маніпулювання почуттям цікавості. Шахраї можуть нібито помилково надіслати урядовцю від імені його керівника електронний лист із вкладенням, яке називається «список_звільнення_жовтень_2020.docx» або «премії_керівників_2020.docx» або «графік_відпусток.docx». Вкладення буде містити шкідливий макрос, який завантажить на комп'ютер вірус.

Співробітники компаній частіше відкривали фішингові листи щодо нібито звільнень, рідше щодо премій чи зарплат та рідко щодо відпусток чи новин щодо актуальних подій в компанії.

3. ЕТАПИ АТАКИ ІЗ ВИКОРИСТАННЯМ СІ:

- розвідка та збір інформації
- легендування атаки
- план атаки
- атака

3.1. РОЗВІДКА ТА ЗБІР ІНФОРМАЦІЇ ІЗ ВІДКРИТИХ ДЖЕРЕЛ

Яка інформація може цікавити хакера?

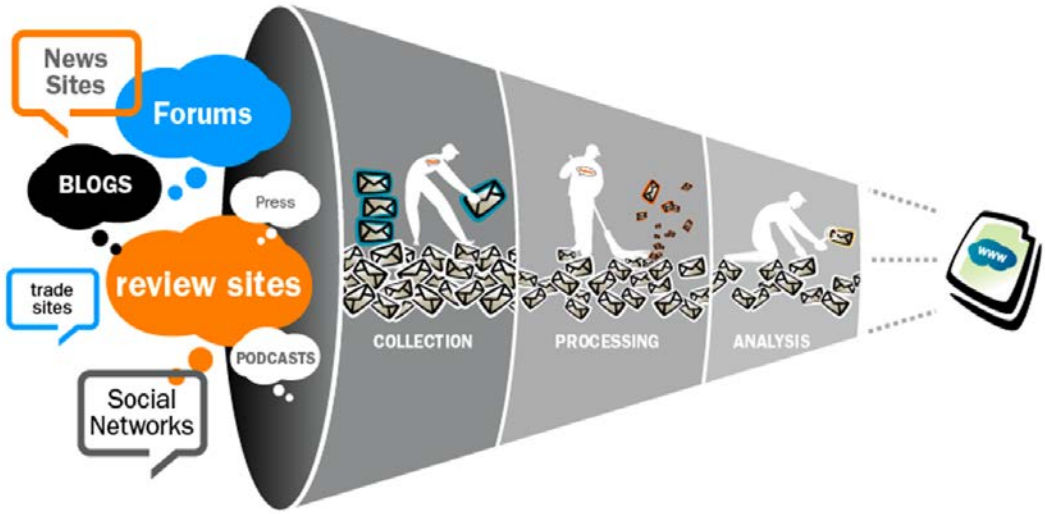
Якщо це стосується конкретної особи, урядовця, співробітника:

- наявність акаунтів в соціальних мережаї;
- емейли, номери телефонів та адреси інтернет-месенджерів;
- деталі щодо сімейного стану, дітей, дружини/чоловіка, батьків тощо;
- місце роботи, заняття, хобі, як проводить вільний час, відпустку;
- деталі щодо посади, як давно працює у компанії/установі, чи задоволений місцем праці, посадою тощо;
- наявність автотранспорту, нерухомості, іншого майна;
- соціальна та громадська діяльність.

Якщо це стосується компанії чи державної установи:

- як побудована мережева інфраструктура (наприклад, чи використовуються групові політики), яким чином здійснюється доступ до мережі «Інтернет»;
- чи використовують (яке?) антивірусне програмне забезпечення;
- версія операційної системи;
- як побудований бізнес, партнери компанії та підрядні організації;
- адреси головного офісу чи філіалів.

Для збору даних хакери проводять розвідку відкритих джерел інформації або OSINT (Open source intelligence). Інформація отримується з різних джерел, зіставляється, аналізується та формулюється у «звіт», який хакер використовує для планування та здійснення CI-атаки.

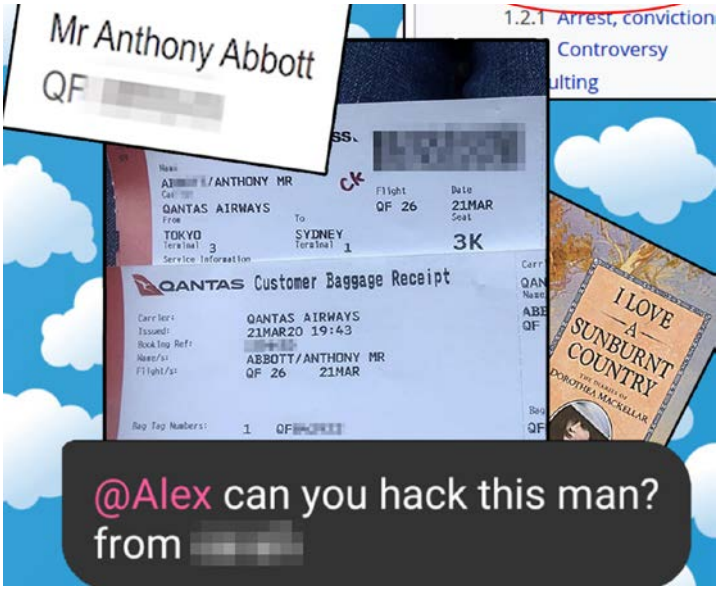


Під час OSINT хакери використовують соціальні мережі, інтернет-месенджери, сервіси електронної пошти, форуми, блоги, сервіси геолокацій, інтернет-мапи, бази даних інформації (як ті, що у вільному доступі, так і з обмеженим доступом).

Кожного року в мережу «Інтернет» потрапляють бази даних популярних соціальних мереж, вебсайтів, онлайн-магазинів тощо. Такі «злиті» бази даних містять різну інформацію щодо користувачів, включаючи їхні логіни або нікнейми, електронні

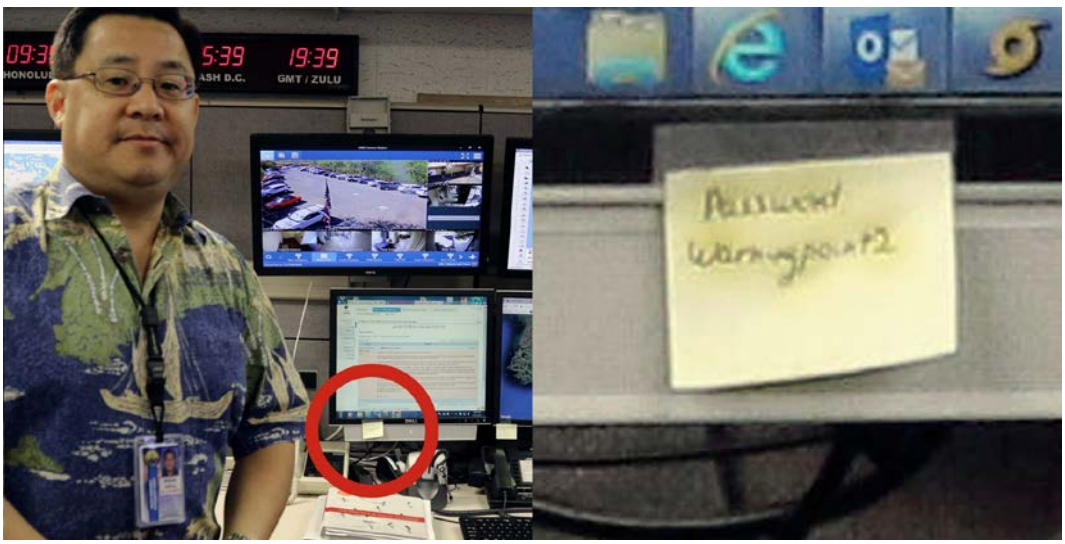
адреси, інтернет-месенджери, інші дані, які користувачі вказували під час реєстрації у ресурсі. Бази даних Adobe, LinkedIn, VKontakte, Badoo, BitTorrent, BTC-E, Comcast, Dropbox та десятка інших ресурсів в різний час потрапили до мережі «Інтернет», тому, якщо Ви користувалися одним із вказаних ресурсів, Ваші персональні дані стали доступними для загального доступу.

Такі злиті бази даних дають хакерам широке поле для планування та здійснення фішингових атак. Сценарії здійснення таких атак обмежуються тільки уявою хакерів. Наприклад, отримавши Ваш старий пароль із бази даних VKontakte, хакер може сформувати фішинговий лист, де вказати цей пароль, як нібито доказ того, що Ваш акаунт було зламано і попросити ввести реквізити доступу до акаунту, як підтвердження, що Ви змінили пароль тощо. Соціальні мережі все ж таки займають домінуюче місце в інструментарії хакера для пошуку інформації щодо своєї майбутньої жертви. В березні 2020 року колишній прем'єр міністр Австралії Tony Abbott у своєму акаунті інстаграму запостив фотографію квитків. Використовуючи ці дані, хакер зміг залогінитися в особистий кабінет Tony Abbott на сайті авіакомпанії та отримати доступ до особистих даних.



(https://www.theverge.com/2020/10/15/21516842/tony-abbott-passport-boarding-pass-instagram-hacking-cybersecurity).

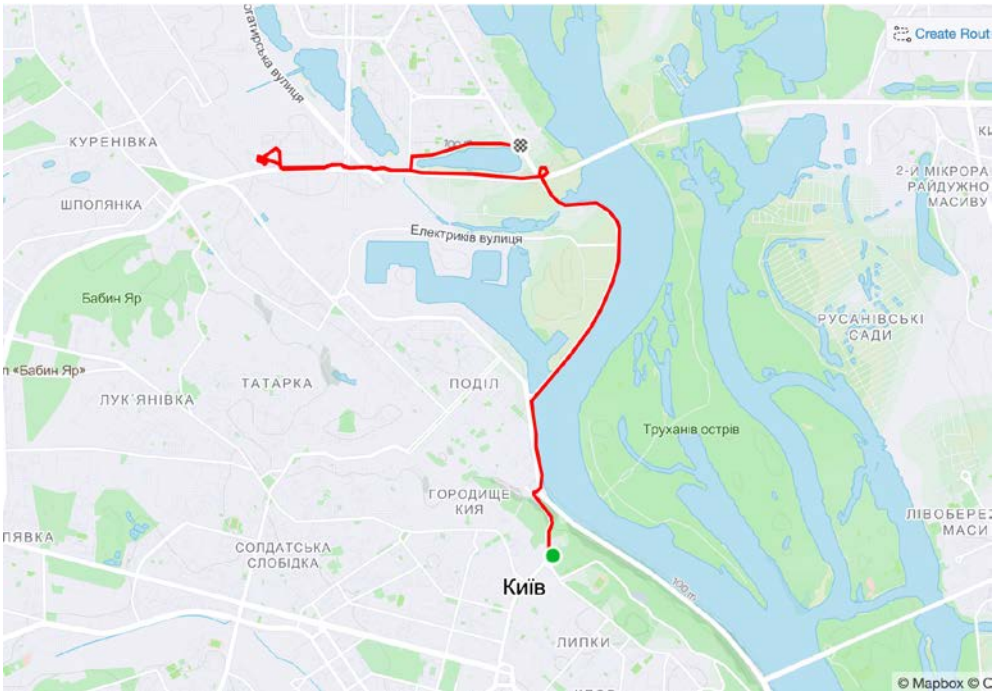
Курйозний випадок стався у 2018 році у Гавайському управлінні Агентства з надзвичайних ситуація США. Співробітник агентства приклеїв на монітор стікер із паролем і його фотографія потрапила в Інтернет:



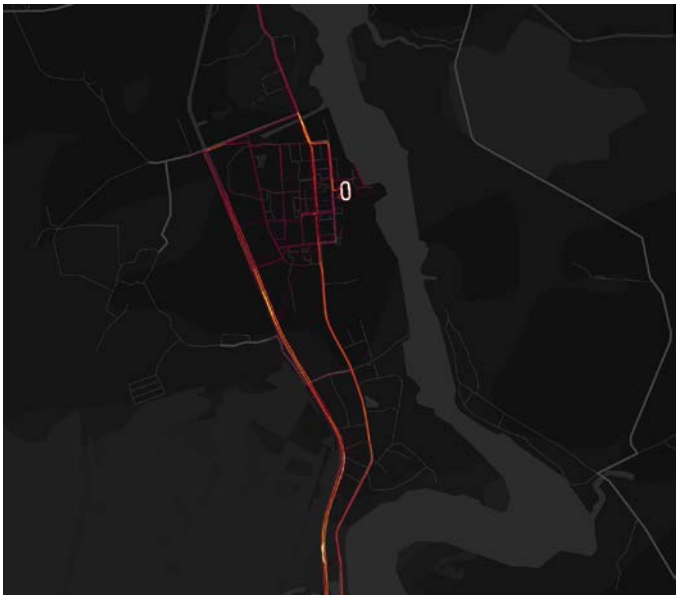
Чи можуть хакери визначити місце Вашого проживання, якщо Ви обмежили користування соціальними мережами та не розміщуєте там свої фотографії?

Так, якщо Ви користуєтесь популярними фітнес-трекерами. Наприклад, фітнес-трекер Strava фіксує усі Ваші тренування, які в подальшому стають доступними для перегляду Вашим контактам, а якщо Ви розміщуєте цю інформацію в соціальних мережах, то вона стає доступною ще більшій аудиторії.

На малюнках, що нижче, видно, де особа розпочинає та закінчує свою велоподорож щодня, що дає уявлення про ймовірне місце її роботи та проживання.



У 2018 році компанія Strava опублікувала глобальну карту використання фітнес-трекерів і тим самим ненавмисно показала місця розташування військових баз США. На мапах Африки та Близького Сходу за сотні кілометрів від населених пунктів можна було побачити візерунки, залишені фітнес-трекерами військових, які займалися на стадіонах та спортивних майданчиках.



Розміщуючи фото в мережі Інтернет не забувайте про метадані фотографії (метадані – це службова інформація, доступна у кожному файлі, яка вказує, коли, як, ким було створено тощо). Якщо йдеться про фотографії, то вони можуть містити географічні координати, де було зроблено фотографію (аналогом є геотеги у соціальних мережах), що значно спрощує хакерам завдання із пошуку та аналізу інформації про свою жертву.

▶ *Про що може розповісти геолокація?*

- де людина любить снідати, обідати, вечеряти;
- в який спортзал ходить;
- де відпочиває, де працює;
- де проводить дозвілля;
- тощо.

Цікавим прикладом використання OSINT для збору інформації про особу є стаття, опублікована на сайті інтернет-видання "Bellingcat" (https://ru.bellingcat.com/materialy/casestudies/2019/04/05/holland-most-wante). "Bellingcat" на базі аналізу фотографій розміщених у соціальних мережах змогло визначити точне місце розташування злочинця-втікача, який переховувався від поліції Нідерландів.

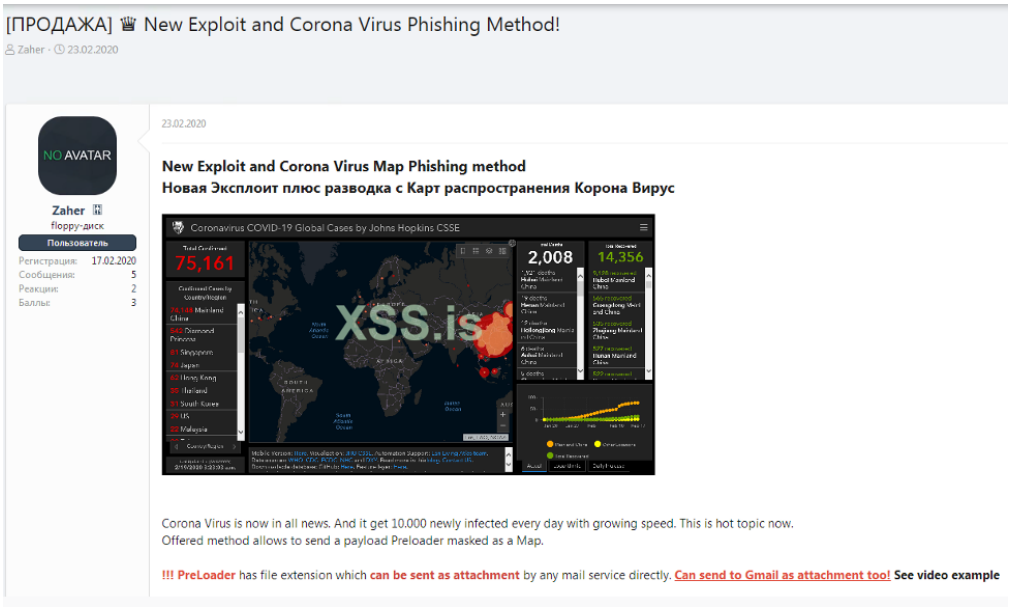
Злочинець активно постив фотографії в соціальних мережах, знущаючись із поліції, закликаючи «зловіть мене, якщо можете».

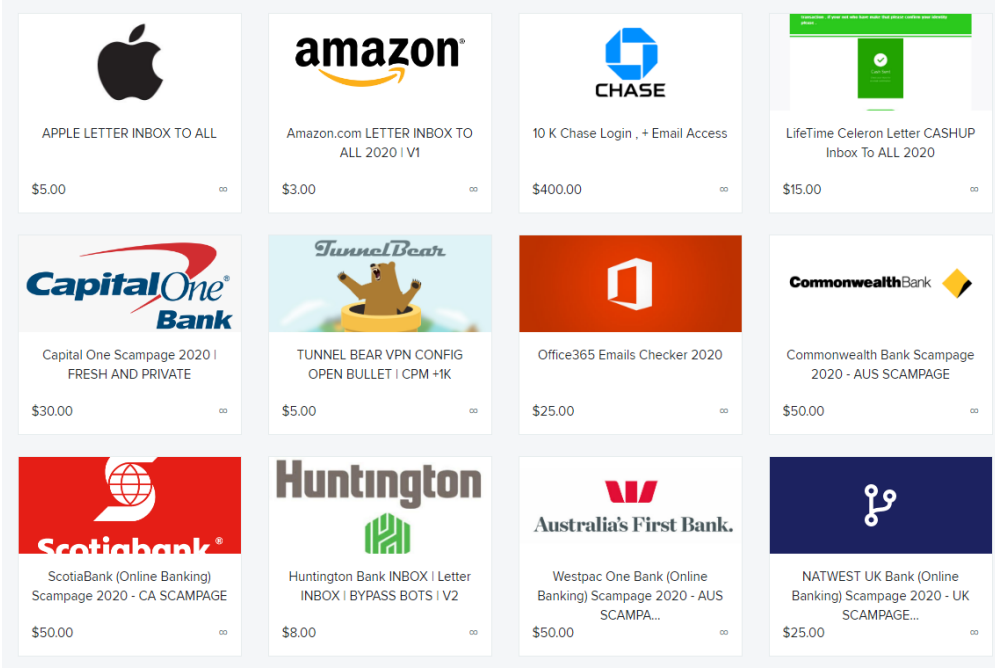

27 nov 2018

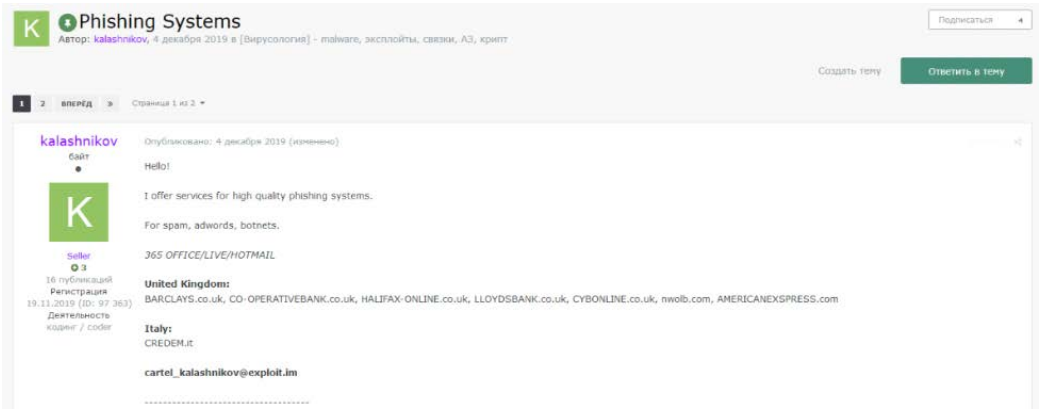
Проаналізувавши десятки фотографій та зіставивши отриману інформацію із відкритими джерелами, фахівцям вдалося встановити будинок, де проживав злочинець, на острові Киш в Персидському заливі.

3.2. ЛЕГЕНДУВАННЯ ТА ПЛАНУВАННЯ АТАКИ ІЗ ВИКОРИСТАННЯ МЕТОДІВ СІ

Легендування та планування атаки із використання методів СІ – не менш важливий етап у її здійсненні. На цьому етапі хакер підготує весь необхідний інструментарій: створить фішинговий лист, напише текст (на практиці це зазвичай роблять спеціальні сервіси і хакери купують фішинговий пакет «під ключ»). На малюнку нижче Ви бачите приклади продажу фішингових пакетів «під ключ».

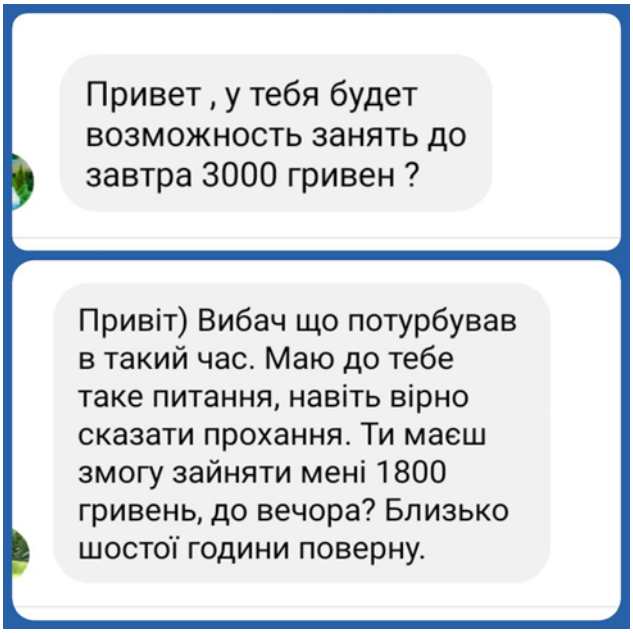

[ПРОДАЖА] ♛ New Exploit and Corona Virus Phishing Method!
Zaher · 23.02.2020
NO AVATAR
Zaher
floppy-диск
Пользователь
Регистрация: 17.02.2020
Сообщения: 5
Реакции: 2
Баллы: 3
23.02.2020
New Exploit and Corona Virus Map Phishing method
Новая Эксплоит плюс разводка с Карт распространения Корона Вирус
Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE
75,161
2,008
14,356
XSS.is
Corona Virus is now in all news. And it get 10.000 newly infected every day with growing speed. This is hot topic now.
Offered method allows to send a payload Preloader masked as a Map.
!!! PreLoader has file extension which can be sent as attachment by any mail service directly. Can send to Gmail as attachment too! See video example


APPLE LETTER INBOX TO ALL
$5.00
Amazon.com LETTER INBOX TO ALL 2020 | V1
$3.00
10 K Chase Login , + Email Access
$400.00
LifeTime Celeron Letter CASHUP Inbox To ALL 2020
$15.00
Capital One Scampage 2020 | FRESH AND PRIVATE
$30.00
TUNNEL BEAR VPN CONFIG OPEN BULLET | CPM +1K
$5.00
Office365 Emails Checker 2020
$25.00
Commonwealth Bank Scampage 2020 - AUS SCAMPAGE
$50.00
ScotiaBank (Online Banking) Scampage 2020 - CA SCAMPAGE
$50.00
Huntington Bank INBOX | Letter INBOX | BYPASS BOTS | V2
$8.00
Westpac One Bank (Online Banking) Scampage 2020 - AUS SCAMPA...
$50.00
NATWEST UK Bank (Online Banking) Scampage 2020 - UK SCAMPAGE...
$25.00



На етапі легендування та планування хакер зазвичай створить та «розкрутить» акаунт в соціальних мережах, з якого запланував здійснити атаку тощо.

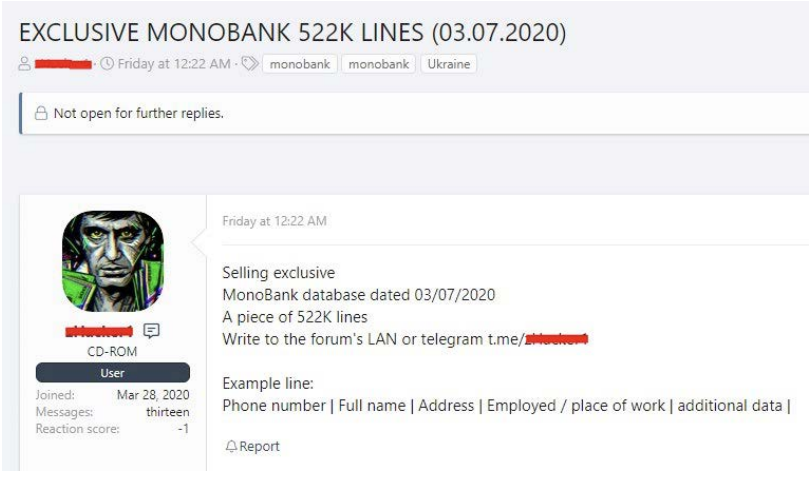
Доволі часто хакери не створюють акаунти, а купують зламані «прокачані» акаунти або самі зламують акаунти, які в подальшому використовують для шахрайства.



Для здійснення фішингової атаки на державні установи хакер може завчасно купити базу даних емейлів державних установ та здійснити на них фішингову розсилку. Чи, навпаки, плануючи атаку, хакер може купити доступ до зламаних акаунтів

електронної пошти державних службовців чи працівників корпоративного сектору та вже з них здійснити фішингову розсилку контрагентам, партнерам та іншим адресатам зламаного ящика електронної пошти. Саме за таким принципом діють деякі банківські трояни. Наприклад, вірус «Анубіс», який атакував мобільні телефони під управлінням операційної системи «Андроїд», розсилав СМС-повідомлення всім абонентам із телефонної книги жертви, таким чином, імовірність того, що абонент відкриває фішингове посилання в повідомленні, отриманому зі знайомого номеру, значно зростає. За схожим принципом діє банківський троян «Емотет». Потрапивши на комп'ютер жертви, вірус не тільки розсилає усім контактам інфікованого акаунту фішингові листи із шкідливим вкладенням нібито від імені інфікованого, але й застосовує іншу тактику, яка називається «викрадення листування» (Eng. email thread hijacking). За такою схемою, вірус викрадає контент емейлу, який знаходиться у папці «Вхідні» та «відповідає» на нього, однак у додаток вставляє шкідливий код. Таким чином, особа, яка отримує такий емейл, думає, що він надійшов у відповідь на раніше надісланий емейл, та, нічого не підозрюючи, відкриває його та запускає вірус.

Очевидно, готуючись до фішингової атаки на клієнтів банків, хакерам доцільно придбати «злиті» бази даних банків чи кредитних установ, щоб вдало побудувати свою лінію поведінки із жертвою. До прикладу, телефонуючи Вам від імені нібито працівника банку, шахрай може значно підвищити рівень довіри до себе, якщо володітиме інформацією про ваші колишні кредити чи рахунки.



Приклад продажу нібито бази даних користувачів «Монобанку» на хакерському форумі.

Загальні поради щодо протидії атакам із використанням СІ

- Не повідомляйте свої персональні дані чи дані про установу, де ви працюєте (її структуру, програмне забезпечення, керівників, іншу службову інформацію) іншим особам, якщо ви не впевнені, що особа, яка запитує цю інформацію, уповноважена чи має право нею володіти.
- Уникайте або обмежуйте публікування своїх персональних даних, фотографій в соціальних мережах, на сайтах чи порталах. Ужодному разі не використовуйте адресу робочої електронної пошти для реєстрації в соціальних мережах чи сайтах, не пов'язаних з роботою, наприклад, в інтернет-магазинах. Якщо це дозволяє, обмежте доступ до вашої сторінки у соціальних мережах лише друзям.
- Якщо сам емейл чи телефонний дзвінок, який Ви отримали, а також саме прохання телефонуючого чи автора емейлу викликає у Вас підозру, перевірте легітимність емейлу чи самого запиту. Ніколи не використовуйте контактні дані, вказані у емейлі, пошукайте інформацію щодо компанії, яка надіслала Вам запит, в інтернеті, звірте логотип, адресу вебсайту, емейл-адресу, номери телефонів тощо. Якщо Ви отримали емейл від Вашого керівника про переказ значної суми грошей на вказаний в емейлі рахунок, а раніше Ваш керівник зазвичай давав такі вказівки усно чи, наприклад, по телефону, зателефонуйте йому та уточніть вказівку.
- Якщо Вам телефонують з невідомого номеру або невідома особа і представляється співробітником банку, поліції, прокуратури тощо та просить повідомити персональні дані, переказати кошти чи повідомити дані платіжної картки – не робіть цього!!! Зазвичай це шахраї. Не піддавайтесь паніці.
- Ігноруйте запити та повідомлення в соціальних мережах від акаунтів, які не мають активності, або помітно, що це одноденні акаунти без постів, з малою кількістю світлин тощо.
- Користуйтесь антивірусами, ліцензійним програмним забезпеченням.
- На всіх сервісах, де це можливо, активуйте двохфакторну аутентифікацію.

Якщо Ви стали жертвою атаки із використанням прийомів СІ

- Якщо Ви помітили підозрілу активність щодо себе, Вам надсилають фішингові емейли, Ви отримуєте підозрілі дзвінки, якщо Ви повідомили сторонній особі службову інформацію, **повідомте про це свого керівника.**
- Якщо Ви повідомили сторонній особі свої особисті дані, реквізити банківської картки чи рахунка, розкрили свій пароль, перейшли за підозрілим посиланням і там залишили згадані вище персональні дані, **негайно змініть паролі та увімкніть двохфакторну аутентифікацію.**
- Слідкуйте в подальшому за своїми акаунтами в соціальних мережах, електронною поштою, банківським рахунком тощо щодо будь-яких підозрілих дій.

МОДУЛЬ № 2:

БЕЗПЕЧНЕ КОРИСТУВАННЯ МЕРЕЖЕЮ «ІНТЕРНЕТ»

МОДУЛЬ № 2: БЕЗПЕЧНЕ КОРИСТУВАННЯ МЕРЕЖЕЮ «ІНТЕРНЕТ»

Доступ до мережі «Інтернет» став одним з основних прав людини. Ми користуємось мережею для дозвілля, розваги, роботи, а також забезпечення повсякденного буття – від оплати рахунків до замовлення послуг.

Вже залишився позаду той час, коли зловмисники використовували мережу лише для розваги або помсти. Зараз ціль будь-якого зловмисника-хакера – гроші. Кожного з них, перш за все, цікавить фінансова вигода. Тобто дії зловмисних програм, а також спеціальних шкідливих або зламаних чи скомпрометованих сайтів, спрямовані на те, щоб заробити на користувачі. А якщо на вас заробляють, то ви особисто обов'язково щось втратите: гроші, час, репутацію.

Найпоширеніші способи нелегального заробітку в мережі «Інтернет» такі:

- Програми-вимагачі – повністю або частково блокують ваш комп'ютер та вимагають оплату для розблокування.
- Викрадення облікових записів соціальних мереж «Фейсбук», «Твітер», «Інстаграм» тощо для розсилки спаму всім вашим друзям або шантажу з приводу повернення вашої сторінки.
- Викрадення поштових даних – як самої електронної скриньки, так і листів, що знаходяться на комп'ютері, в яких міститься інформація про ваші реєстраційні дані на інших ресурсах.
- Використання комп'ютера у складі bot-net – на тисячі комп'ютерів завантажуються шкідливе програмне забезпечення, яке застосовується для масової розсилки спам-повідомлень або для атаки інших ресурсів.
- Викрадення даних, які мають відношення до фінансових операцій: особиста документація, кредитні картки та інші платіжні системи.
- Несанкціонований показ рекламних повідомлень.

Проте що може статись, коли метою атаки є не людина, а інформаційна система міста, органу державної влади або іншої важливої установи? Насправді, людина стає тією ланкою, яка призводить не тільки до репутаційних та особистих майнових втрат, але й каталізатором критичних, а іноді й катастрофічних ситуацій.

Наприклад, у липні 2019 року влада міста Лейк-Сіті (штат Флорида, США) заплатила хакерам викуп у розмірі $ 460 тис. Муніципальні комп'ютерні системи Лейк-Сіті були заражені 10 червня. Вірус зашифрував усі дані, що зберігаються в інформаційних системах міської адміністрації. Незабаром хакерське угруповання, що провело кібератаку, запросило викуп в розмірі 42 біткойнов. Адміністрація міста оцінила витрати, пов'язані з можливою втратою даних, і вирішила виплатити необхідну суму. Після того, як хакери отримали необхідний викуп (на момент виплати близько $ 460 тис.), адміністрації міста був переданий ключ для дешифрування даних. Робота міських інформаційних систем була відновлена, а один із співробітників відділу технічного забезпечення муніципальної адміністрації був звільнений. Але чи відшкодувало звільнення винної особи витрати платників податків? Авжеж ні! Проте чи поодинокі такі випадки? Ні!

За місяць до описаного випадку адміністрація міста Рів'єра-Біч (штат Флорида, США) виплатила $ 600 тис. хакерам, які захопили міську комп'ютерну інфраструктуру. Комп'ютерна мережа адміністрації американського курортного міста була атакована за допомогою вірусу-шифрувальника в кінці травня. Кібератака вразила безліч урядових систем, включаючи службу порятунку 911 – диспетчери не могли вводити інформацію про вхідні виклики в комп'ютерну програму. Тобто питання вже не тільки про доступ до інформації, але й про життя громадян. І це вже стає реальністю.

Хакерська атака на лікарню міста Дюссельдорф призвела до смерті пацієнтки восени 2020 року. Жінку, якій знадобилася термінова госпіталізація, не прийняли в госпіталь через злам комп'ютерних систем і відправили в сусіднє місто Вуппераль, що знаходиться в 32 км. Через те, що час для порятунку було упущено, пацієнтка померла.

Але що було причиною? В усіх трьох випадках першоджерелом атаки була помилка або недбалість посадової особи: від випадкового відкриття листа з шкідливим вкладенням до неналежного нагляду за програмним забезпеченням.

Яким чином це все відбувається? Наприклад, програма, яка була завантажена Вами з недостовірних джерел мережі «Інтернет» або запущена зі знайденого USB-носія, виходить у Всесвітню Мережу та завантажує троянську програму. Не одну. Зазвичай подібні загрози поширюються на комп'ютері як грибниця – там, де одна,

там і інша. Цим самим зловмисники страхують себе від того, що існуючий антивірус зможе видалити всі небезпечні програми. Зрозумійте, що нові зразки шкідливого програмного забезпечення з'являються постійно, навіть автоматично, тобто генерують самі себе. Тож з великою вірогідністю один запуск програми-оманки – і 1-2-3-4 загрози залишаться на комп'ютері, як би Ви його не перевіряли, і будуть виконувати свою роботу, паралельно завантажуючи нових «братів» та активуючі необхідні функції.

І це не обов'язково починається із завантаження Вами підозрілої програми. Все може починатися інакше і «елегантно». Ви переглядаєте сторінки в інтернеті і в одну мить переходите за посиланням на небезпечний сайт або відомий сайт чомусь перенаправив вас на інший. З вигляду він може нічим не відрізнятися від інших сайтів і нести цікаву чи корисну інформацію – ніхто вас не попередить ні про загрозу, ні про її наслідки. Із сайту, використовуючи вразливості Вашого браузеру чи його додатків, на ваш комп'ютер без Вашої згоди (або взагалі інформування) таємно завантажується крихітна програма, яка у свою чергу скачує та інсталює вищезазначені загрози.

До аналогічного результату може призвести зовнішня атака на ваш комп'ютер, як цільова – хакером, так і випадкова – таким же bot-net, частиною якого можете стати ви. Давайте розберемось, як це відбувається, та яким чином захиститись від цих загроз.

БЕЗПЕКА БРАУЗЕРІВ

Що таке інтернет-браузер? Це програмне забезпечення, яке дозволяє користувачам отримувати інформацію з сайтів мережі «Інтернет». Браузери транслюють код інтернет-сторінок у зрозумілий людині вигляд. Для передачі використовується протокол HTTP або його безпечніша версія HTTPS. Протокол – це набір правил передачі файлів (тексту, зображень, відео тощо) через мережу «Інтернет». Приклади браузерів: "Google Chrome", "Mozilla Firefox", "Microsoft Edge", "Apple Safari", "Internet Explorer".

Але браузери наразі не тільки надають доступ до сторінок, але і слугують платформою для додаткових програм, які полегшують користування мережею «Інтернет». Ці програми мають назву – плагіни. Плагіни розширюють функціональність браузеру, додаючи додаткових функцій. Більшість плагінів можуть встановлювати додаткові панелі інструментів, маркетинг і помічників пошуку. Крім того, ви може помітити нові кнопки, посилання або функції, такі як блокування спливаючих вікон, доданих в браузер. Деякі плагіни невидимі для користувача, оскільки вони працюють у фоновому режимі і не мають графічного інтерфейсу. Деякі з плагінів можуть бути шкідливими. Щоб пам'ятати Вас, браузери використовують таку річ, як cookies.

Cookies – це невеликі текстові файли у нас на комп'ютерах, в яких зберігається інформація про Ваші попередні дії на сайтах. Крім входів в акаунти, вони вміють запам'ятовувати:

- налаштування користувачів, наприклад, мова, валюта або розмір шрифту;
- товари, які ми переглядали або додали в кошик;
- текст, який ми вводили на сайті раніше;
- IP-адресу і місце розташування користувача;
- дату і час відвідування сайту;
- версію ОС і браузера;
- кліки та переходи.

Коли ми робимо на сайті якась дії, наприклад, додаємо товар в корзину або вводимо дані входу в аккаунт, сервер записує цю інформацію в cookies і відправляє браузеру разом зі сторінкою. Коли ми переходимо на іншу сторінку сайту або заходимо на нього через час, браузер відправляє cookies назад.

Cookies бувають тимчасовими і постійними. Постійні cookies залишаються на комп'ютері, коли ми закриваємо вкладку з сайтом, а тимчасові видаляються. Які саме cookies використовувати на конкретному сайті – тимчасові або постійні – вирішує його розробник. Саме тому на одних сайтах ми не виходимо з акаунтів, навіть коли заходимо на них раз через кілька днів, а на інших вводимо пароль заново, хоча відійшли від комп'ютера на п'ять хвилин.

Самі по собі cookies не є небезпечними – це звичайні текстові файли. Вони не можуть запускати процеси на комп'ютері та взагалі взаємодіяти з операційною системою.

Але їх можуть спробувати перехопити або вкрасти, щоб відстежити ваші попередні дії в мережі або входити у ваші акаунти без авторизації.

Зазвичай інформацію, яку записують в cookies, зашифровують перед відправкою, а самі cookies передають за HTTPS-протоколом. Це допомагає захистити призначені для користувача дані, але за впровадження шифрування і безпечну відправку відповідає розробник сайту. Відвідувачам залишається тільки сподіватися, що все налаштували грамотно. Зі свого боку користувач може тільки заборонити браузеру використовувати cookies або час від часу чистити їх самостійно.

Зовсім відключати cookies – не завжди хороша ідея. Наприклад, всі інтернет-магазини працюють за допомогою cookies. Якщо заборонити браузеру їх використовувати, сервер не зможе запам'ятати, що саме ви додали в кошик. Чистити cookies вручну практичніше, але доведеться щоразу заново налаштовувати зовнішній вигляд сайту і входити в акаунти.

Чому через браузер можуть реалізовуватись загрози?

- Браузери застарівають та з'являються вразливості, які експлуатуються хакерами віддалено.
- Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, і Ви можете навіть не знати про те, що стали жертвою.
- Зловмисники зламують публічні точки доступу до мережі «Інтернет» і намагаються перехопити інформацію користувачів

Якщо Ви звернете увагу на новини зі світу кібербезпеки, то побачите, що браузери майже щомісяця публікують оновлення та звітують про винайдені та закриті вразливості. Чому? Тому що дуже велика кількість вразливостей виявляється ледь не щоденно. І хакери одразу починають їх використовувати у своїх атаках.

Треба зрозуміти, що не існує абсолютно безпечного браузеру. Іноді виникає ситуація, коли вразливості можуть залишатися незакритими протягом десятиріч. Наприклад, незалежний експерт з кібербезпеки Барак Тавілі (Barak Tawily) виявив спосіб, за допомогою якого зловмисники протягом 17 років могли отримувати доступ до файлів на комп'ютері через вразливість в браузері "Mozilla Firefox".

Тобто Ви, щоб не ставати жертвою, маєте ретельно піклуватись про безпеку вашого браузера. Але треба пам'ятати, що Ваша необачність може нести ризики не тільки Вам особисто, але й усій Вашій установі.

Як Вам убезпечити браузер?

- Необхідно постійно оновлювати браузер, щоб не допустити появи відомих вразливостей у ньому.
- Також Вам необхідно коректно налаштувати вимоги до приватності ваших даних у браузері.
- Встановити додаткові плагіни безпеки, наприклад, HTTPS Everywhere (буде попереджати, якщо сайт не захищено HTTPS і є ризик перехоплення даних: логінів, паролів тощо) або AdBlock (блокувальник реклами).

"GOOGLE CHROME"

Функцію виявлення фішингу та зловмисного програмного забезпечення ввімкнено за замовчуванням. Якщо її ввімкнено, можуть з'являтися перелічені нижче повідомлення. Якщо ви бачите одне з них, радимо не переходити на такий сайт.

- Сайт містить зловмисне програмне забезпечення. Сайт, на який ви хочете перейти, може спробувати встановити на ваш комп'ютер зловмисні програми.
- Оманливий сайт. Сайт, на який ви хочете перейти, підозрюється у фішингу.
- Підозрілий сайт. Сайт, на який ви хочете перейти, здається підозрілим і може бути ненадійним.
- Сайт містить шкідливе програмне забезпечення. Сайт, на який ви хочете перейти, може оманливим шляхом змусити вас встановити програми, які спричиняють проблеми під час роботи в інтернеті.
- Ця сторінка намагається завантажити скрипти з неперевірених джерел. Сайт, на який ви хочете перейти, ненадійний.
- Можливо, ви мали на увазі [назва сайту]? або Це потрібний сайт? Сайт, на який ви намагаєтеся перейти, може насправді бути не тим, який ви хочете відкрити.

Важливо: перевіряйте вміст, який завантажуєте. Деякі сайти повідомляють, що на пристрої є вірус, щоб обманом змусити вас завантажити шкідливе програмне забезпечення. Не робіть цього.

Як встановити плагін

- Відкрийте інтернет-магазин "Chrome".
- Знайдіть потрібний плагін (розширення).
- Натисніть «Встановити».
- Деяким розширенням можуть знадобитися дозвол або доступ до певних даних. Щоб надати доступ, натисніть «Додати розширення».

Увага! Схвалювати слід тільки надійні розширення.

- Щоб почати роботу з розширенням, натисніть на його значок праворуч від адресного рядка.

Як управляти розширеннями

- Відкрийте Chrome на комп'ютері.
- У правому верхньому куті вікна натисніть на значок «Налагодження та управління Google Chrome», потім «Додаткові інструменти», потім «Розширення».
- Внесіть зміни.
- Увімкніть або вимкніть розширення.
- Дозвольте використовувати в режимі інкогніто. Для цього натисніть кнопку Детальніше, а потім встановіть відповідний перемикач в потрібне положення.
- Виправте пошкодження. Якщо розширення не працює, натисніть «Відновити», а потім «Відновити розширення».
- Дозвольте доступ до сайтів. Поруч з розширенням натисніть «Детальніше». У пункті «Дозволити розширенню перегляд і зміну ваших даних на відвідуваних сайтах» виберіть «При натисканні», «На обраних сайтах» або «».

"MOZILLA FIREFOX"

Панель «Приватність» дозволить вам:

- Контролювати те, як «Фаєрфокс» оброблятиме вашу історію, яка включає: відвідані вами сторінки, завантажені файли, введені дані в текстові поля на сторінках та встановлені сайтами cookies.
- Керувати тим, які сайти можуть надсилати вам cookies та вилучати вже встановлені сайтами cookies.
- Керувати тим, як панель «Адреса» використовуватиме історію для пропонування вам підказок під час друкування в ній.

Панель «Безпека» містить опції щодо безпеки вашого перебування у мережі.

Видавати попередження у разі спроби вебсайтів встановити додаток: «Фаєрфокс» завжди запитуватиме у вас підтвердження на встановлення додатків. Задля запобігання небажаного запиту на встановлення, який випадково може призвести до встановлення додатку – «Фаєрфокс» попереджатиме вас у разі спроби вебсайту встановити додаток і блокуватиме такий запит на встановлення.

Повідомити мене, якщо відвідуваний сайт відзвітований як нападник: позначте цю опцію якщо ви хочете, щоб «Фаєрфокс» перевіряв, чи може відвідуваний вами сайт перешкоджати нормальній роботі вашого комп'ютера або надсилати особисті дані про вас не уповноваженим на це третім сторонам в інтернеті.

Блокувати сайти, відзвітовані як нападники: позначте цю опцію, якщо ви хочете, щоб «Фаєрфокс» перевіряв, чи може відвідуваний вами сайт перешкоджати нормальній роботі вашого комп'ютера або надсилати особисті дані про вас не уповноваженим на це третім сторонам в інтернеті.

Повідомити мене, якщо відвідуваний сайт відзвітований як підробка: вказує «Фаєрфокс» перевіряти, чи вводить відвідуваний вами сайт вас в оману задля отримання вашої персональної інформації (даний процес також відомий під словом фішинг).

Блокувати сайти, відзвітовані як підробки: вказує «Фаєрфокс» перевіряти, чи вводить вас в оману відвідуваний вами сайт задля отримання вашої персональної інформації (даний процес також відомий під словом фішинг).

Зауважте, відсутність такого повідомлення не гарантує, що цьому сайту можна довіряти.

БЕЗПЕКА ДАНИХ

Треба розуміти, що Ви відповідальні за безпеку не тільки Вашого комп'ютера, але й даних, якими Ви володієте або керуєте. Ті дані, які зберігаються на Вашій робочій станції мають бути захищені не тільки антивірусним захистом, але й наявністю резервних копій та розмежуванням доступу, але про це пізніше.

Щодо даних, які Ви вводите на різних сайтах мережі «Інтернет» під час реєстрації або використання, то запам'ятайте одне: те, що ви відправили в мережу, вже Вам не належить. Інформація може бути вкрадена, скомпрометована, підроблена або знищена навіть без Вашого відома, не кажучи вже про дозвіл.

Наполегливо рекомендуємо не вводити персональні дані (логін, пароль, номер телефону чи платіжної картки) на запити не перевірених або підозрілих сайтів. Який сайт підозрілий? Той, який Ви бачите вперше!

Дані можна надавати лише тим ресурсам, які вже пройшли Вашу перевірку або відомим мережам (наприклад, "Google", "Facebook", "Rozetka", "Twitter" та інші). І ще – обов'язково перевіряйте назву сайту в адресному рядку браузера (www.rozetka.ua, а не rozetka.ug або rozteka.com.ua). Вводити ж інформацію з платіжних карток чи паролі від них можна лише на сайтах зі знаком «замочка» в адресному рядку. Таке з'єднання вважається захищеним, а ваші дані не потрапляють до рук сторонніх осіб, які можуть отримати доступ Вашої комунікації з інтернет-сторінкою. Як вони можуть отримати доступ? Наприклад, за допомогою зламу Wi-Fi. Але про це трохи згодом.

Щодо робочої адреси електронної пошти, телефону та іншої офіційної інформації, то є одна порада: не використовувати ці дані ніде, крім офіційних джерел. Особливо не радимо використовувати робочі засоби комунікації: номер телефону або адресу пошти для особистих питань. Ризики цього – надвисокі! Хакери полюють за такими даними та використовують їх потім для спроб атак на установи.

Пам'ятайте: як посадова особа, Ви відповідальні не тільки за себе, але й за інших!

БЕЗПЕЧНЕ КОРИСТУВАННЯ МЕРЕЖАМИ WI-FI

2017 року фахівці з "Avast" провели експеримент над відвідувачами "Mobile World Congress". Вони створили три відкриті Wi-Fi точки біля стенду для реєстрації відвідувачів виставки в аеропорту і назвали їх стандартними іменами "Starbucks", "MWC Free WiFi" і "Airport_Free_Wifi_AENA". За 4 години до них підключилися 2000 чоловік.

За підсумками експерименту була зроблена доповідь. Фахівці змогли проаналізувати трафік всіх цих людей і дізнатися, які сайти вони відвідували. Також дослідження дозволило дізнатися особисту інформацію 63% учасників: логіни, паролі, адреси електронної пошти тощо. І жертви ніколи б не дізналися про те, що їх дані потрапили в руки до когось ще, якби експерти з "Avast" не розкрили свій секрет.

Більшість людей, що підключилися, були технічно освіченими. Адже вони приїхали на міжнародну IT-виставку. Але чомусь вони не вживали жодних заходів із самозахисту під час використання публічного Wi-Fi.

Нижче ви дізнаєтеся, чим може загрожувати підключення до безкоштовного Wi-Fi і як захистити себе, використовуючи його. Почнемо з перерахування найпоширеніших небезпек.

Власник Wi-Fi-точки або людина, яка отримала доступ може переглядати весь трафік, який проходить через неї і дізнаватися, на які сторінки люди заходили з підключених пристроїв, що вводили у форми на сайтах, які використовують протокол http. Це можуть бути дані для входу, тексти листів, повідомлення на форумах.

Ще за допомогою аналізатора трафіку можна вкрасти cookie-файл з ідентифікатором сесії, який можна використовувати для входу на деякі сайти під аккаунтом жертви.

Так, наразі більшість популярних сайтів використовують безпечний протокол https, за яким логіни і паролі передаються в зашифрованому вигляді. І їх не можна дізнатися описаним вище чином. Але це не означає, що їх не можна вкрасти за допомогою Wi-Fi мережі.

Коли людина підключається до Wi-Fi в громадському місці, то її можуть направляти на сторінку для підтвердження своєї особи за номером телефону або авторизації через соцмережі. Всі введені на цих сторінках дані власник точки може збирати для особистого користування.

Також людина, у якої є доступ до управління роутером може налаштувати, наприклад, перенаправлення з facebook.com на сайт facebb00k.com, на якому буде розміщена копія головної сторінки популярної соцмережі, створена для крадіжки паролів.

Таким же чином людину можна перекидати не тільки на фішингові сайти, але і на сторінки для скачування троянів і вірусів. Результат буде залежати від того, наскільки Ви піклуєтеся про безпеку свого пристрою.

Таким чином, використання Wi-Fi-мереж потребує уважності та знання деяких правил кібербезпеки. Дотримуючись їх ви з високою ймовірністю зможете позбавити себе від крадіжки Ваших персональних даних, паролів, логінів, грошей з банківських рахунків. Будьте уважні і на роботі. “McDonalds” раптово та швидко поруч не відкривається!

ОСНОВНІ ПРАВИЛА БЕЗПЕЧНОГО КОРИСТУВАННЯ WI-FI

Ці правила стосуються всіх видів пристроїв: ПК, планшетів, смартфонів:

1. Встановити антивірус або комплексну програму безпеки;

2. Вимкнути функцію автоматичного виявлення та підключення до доступних мереж;

3. Не робити жодних грошових операцій: перекази, покупки, регулярні платежі у публічних мережах;

4. Не вимикати брандмауэр або файрвол;

5. Використовувати безпечний протокол з’єднання HTTPS та перевіряти його наявність в браузері;

6. Вимкнути загальний доступ до файлів і папок у вашій операційній системі;

7. І якщо все ж таки є необхідність зробити критичну дію, то користуватися сервісами VPN.

Дотримуйтесь цих правил, і використання громадських Wi-Fi мереж буде максимально безпечним для Вас.

Firewall (фаєрвол або фаєруол), він же – мережевий екран – це загальна назва програмних або апаратних бар'єрів (екранів) для захисту комп'ютерів, мережевих пристроїв або цілих мереж від несанкціонованого доступу ззовні.

Усі мережеві екрани, загалом, працюють як фільтри для вхідного і вихідного трафіку. Також вони можуть надавати розширені функції з управління фільтрацією трафіку за адресами і номерами портів, видавати повідомлення про прецеденти порушення безпеки тощо.

Функціональність мережевих екранів від різних виробників може відрізнятися, але основне завдання вони всі вирішують одне – фільтрація трафіку і блокування несанкціонованого доступу до пристрою, комп'ютера або інших мережевих ресурсів.

Так, на сьогоднішній день, комп'ютер, не захищений мережевим екраном (фаєрволом), за статистикою, при підключенні до інтернету, буде заражений вірусами або іншими шкідливими програмами за лічені хвилини. Практично всі сучасні операційні системи постачаються з вбудованими мережевими екранами. Тому рекомендуємо вам користуватися, як мінімум, цими інструментами. Наприклад, "Windows" постачається з програмою "Windows Firewall". У "Linux"-системах найбільш популярною є програма "Iptables".

БЕЗПЕЧНЕ КОРИСТУВАННЯ МЕСЕНДЖЕРАМИ

У перекладі з англійської «messenger» означає «гонець», «посланник», «посланець». Словом, «той, хто приносить новини». так що таке месенджери і якими вони бувають? В IT-сфері за месенджером давно закріпилось визначення як програмного засобу для миттєвого обміну короткими повідомленнями по електронних каналах

зв'язку. Зазвичай під каналами зв'язку мається на увазі інтернет, хоча зустрічаються і рідкісні винятки.

Які ризики несе користування месенджерами?

1. Розкриття вашої приватної інформації: від номеру телефону до фотографій та іншого.

2. Шахрайство – шахраї дуже часто користуються саме месенджерами, щоб уникнути виявлення.

3. Розповсюдження шкідливого ПЗ через функції автозавантаження.

У 2017 році була виявлена тенденція – викрадення інформації через месенджери.

У 2018 році кількість витоків інформації через месенджери зросла на 14,3%, хоча раніше цей канал зовсім не виділявся в статистиці. Крім того, постійно виявляються нові модифікації шкідливих програм, що відстежують переписку в популярних месенджерах, таких як "Telegram", "WhatsApp", "Skype" та інших.

Люди все більше і більше діляться особистою інформацією в мобільних додатках: якщо п'ять років тому можна було втратити лише особисті фотографії, то сьогодні це комерційне листування, рахунки в банках, контакти. Розробники додатків часто просто не встигають за хакерами, тому допомогти Вам може лише дотримання правил безпеки.

Як убезпечити себе під час користування месенджерами?

1. НЕ передавайте через месенджер жодну інформацію, розкриття якої для вас небажане.

2. Відключайте автоматичне завантаження файлів, особливо для контактів, що відсутні у вашій адресній книзі.

3. Не переходьте за посиланнями, особливо скороченими, які надійшли від недовірених контактів.

4. Оновлюйте месенджери.

Памятайте про основне: Ваша особиста безпека – це Ваша відповідальність. Але від Вашої безпеки може залежати добробут та майбутнє співробітників, близьких та інших громадян України.

МОДУЛЬ № 3:

БЕЗПЕЧНЕ КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

МОДУЛЬ № 3: БЕЗПЕЧНЕ КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

Кожного дня ми використовуємо електронну пошту для робочих та особистих цілей. Вона стала одним з основних каналів комунікації з нами і тому є неабияк привабливою для кіберзлочинців та інших зацікавлених сторін. Сьогодні ми поговоримо про те, які існують загрози під час використання електронної скриньки та що ми маємо робити, щоб себе захистити.

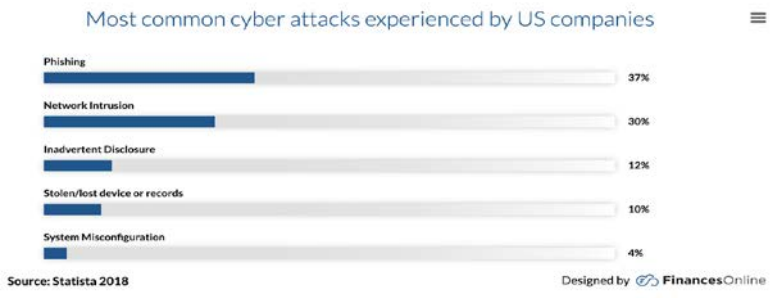
1. НАЙВІДОМІШІ АТАКИ ЧЕРЕЗ ЕЛЕКТРОННУ ПОШТУ

Після того, як люди почали активно користуватись емейлом, історія бачила чимало успішних кібератак, які використовували пошту як інструмент доставки шкідливого програмного забезпечення та виманювання у людей конфіденційної інформації.

- *Вірус **ILOVEYOU** (2001) спричинив близько $10 мільярдів збитків. Було заражено ~ 10% всіх комп'ютерних систем у світі. Злочинці надіслали листи із зізнанням у коханні та скористались людською зацікавленностю, щоб адресати відкрили файл у додатку.*

- *Вірус **MyDoom** (2009) спричинив $38 мільярдів збитків. Користувачі отримували листа нібито з помилкою доставки емейлу до якогось отримувача і деталі помилки знаходились у додатку, прикріпленому до емейлу.*

Знизу на графіку ми бачимо, що 37% з усіх атак здійснюються за допомогою електронної пошти.



ЧОМУ ЕЛЕКТРОННА ПОШТА НАСТІЛЬКИ ПРИВАБЛИВА ДЛЯ КІБЕРЗЛОЧИНЦІВ?

- Бази даних поштових скриньок легко знайти в мережі «Інтернет»;
- Функція додатків до листів дозволяє злочинцям надсилати файли з шкідливим програмним кодом;
- Користувачі не очікують отримати листи зі шкідливими вмістом/ Користувачі часто несвідомо відкривають всі листи, які до них надходять;
- Злочинці користуються людською психологію, щоб збільшити шанси відкриття шкідливих файлів (наприклад маскуючись під…).

Особиста та робоча пошта

Одним з перших правил безпеки електронної скриньки (насправді не тільки її) є чітке розмежування особистого та службового. Але чому це так важливо?

Розгляньмо різницю:

Службова пошта:

- показує вашу належність до організації – (vasyl@**me.gov.ua**). Ми бачимо, що Василь належить до Міністерства розвитку економіки. Тим самим викликає довіру та авторитет до листів, які надходять з цієї адреси;
- дані зберігаються на серверах вашої установи і адмініструються відділом інформаційних технологій. Треті сторони не повинні мати доступ до цих даних;
- містить конфіденційну інформацію, яка стосується вашої організації.

Особиста пошта:

- зберігається на серверах компанії, яка надає послуги поштового сервісу;
- містить вашу приватну інформацію;
- використовується для реєстрації у соціальних мережах та на інших ресурсах.

Підсумок:

Отже, змішуючи особисту та службову пошти:

1. Не знаємо, хто може мати доступ до приватних або службових даних. IT-відділ може бачити вашу особисту переписку, а провайдери поштових сервісів – службову комунікацію.

2. Не контролюємо, до яких ресурсів буде мати доступ злочинець у разі компрометації безпеки вашої скриньки.

3. Збільшуємо ймовірність зламу ваших облікових записів.

Наслідки можуть бути жахливими і саме ваші облікові записи можуть стати інструментом для атаки на вашу організацію.

ЯК СЛІД ВИБИРАТИ, ЯКИЙ ПОШТОВИЙ СЕРВІС ВИКОРИСТОВУВАТИ?

Якщо ми говоримо про особисту пошту, то як же правильно обирати її та що будуть знати про нас провайдери поштового сервісу?

Перш ніж продовжити, ми маємо усвідомити одну істину:

«Якщо ми не платимо за продукт, ми є продуктом (в даному випадку наші дані та інформація, яка проходить через нас)».

Трішки вище, ми з вами говорили про зберігання даних на серверах компаній, які надають послуги з поштового сервісу, таких як: gmail.com, ukr.net, outlook.com, і т.д. Але навіщо їм надавати безкоштовно ці послуги? Вони ж витрачають свої ресурси, зберігаючи наші дані. Відповідь на це - гроші.

ФІНАНСОВИЙ МОТИВ

Так, наприклад, компанія "Google" прописує в своїх політиках, що вони дійсно заробляють на інформації про нас. Ось витяг з цих політик*:

- *«Ми використовуємо ваші особисті дані, щоб зробити сервіси "Google" корисніше для вас, наприклад пропонувати варіанти автозаповнення під час введення пошукових запитів, підбирати оптимальні маршрути на Картах або показувати вам рекламу на основі ваших інтересів».*
- *Ми отримуємо кошти або за розміщення оголошення (наприклад, банера у верхній частині сторінки), або за результати показу, такі як клік по оголошенню".*

ЗАЦІКАВЛЕНІСТЬ ІНОЗЕМНИХ ДЕРЖАВ

Ці техгіганти зберігають мільярди терабайтів інформації про нас, і держави різних країн неабияк зацікавлені у тому, щоб мати ці дані.

Такі компанії, як mail.ru та yandex.ru підвладні державі, в рамках якої вони функціонують, і зливають інформацію про своїх користувачів. Користування ними створює загрозу національному інтересу іншої країни.

Інтереси іноземних держав:

- формування суспільної думки;
- передача даних службам безпеки.

Приклад, як Yandex.ru передала ФСБ інформацію про людей, які фінансово підтримали антикорупційний сайт опозиційного російського політика.

https://www.bbc.com/news/business-13274443.
Рішення ЄСПЛ. Подивитись.

Підсумок:

Отже, коли ви вибираєте поштовий сервіс, необхідно подумати про таке:

- Чи готові ви платити за користування поштовим сервісом?

  Так. Перелік рекомендованих сервісів:
  https://protonmail.com/ua/signup (є безкоштовна опція з лімітом на 500 мб)

  Ні. Усвідомлюйте, що ви будете платити вашими даними.

Якщо вибрали все ж таки платити своїми даними, звертайте увагу на такі критерії:

- З якої країни походить компанія?
- Чи підвладна ця компанія державі?
- Чи була помічена у зливі інформації про своїх користувачів?
- Чи є політичний інтерес у цієї держави?

Тому, такі компанії, як “Yandex”, “Mail.ru”, “Однокласники”, і т.д заборонені законом України, адже вони становлять загрозу українському суспільству.

2. ЯКІ ЗАГРОЗИ ІСНУЮТЬ ПІД ЧАС КОРИСТУВАННЯ ПОШТОВОЮ СКРИНЬКОЮ?

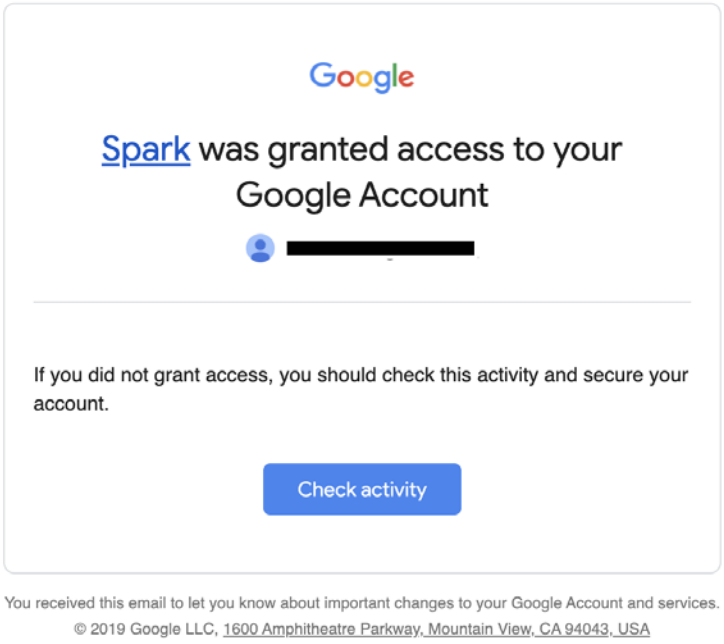
ФІШИНГ. ВИЗНАЧЕННЯ ТА ПРИКЛАД ФІШИНГУ

Фішинг – це схема, за якої хакери змушують користувачів передавати конфіденційну інформацію, наприклад, паролі та номери соціального страхування. Вона зазвичай передбачає надсилання повідомлення спаму, яке справляє враження, ніби походить із довіреного джерела, наприклад, із банку (це наживка). У повідомленні спаму міститься посилання на шахрайський вебсайт, що видається за довірене джерело (це пастка). Користувач, нічого не підозрюючи, вводить інформацію, яка цікавить хакерів, вважаючи, що перебуває на сайті, який заслуговує на довіру.

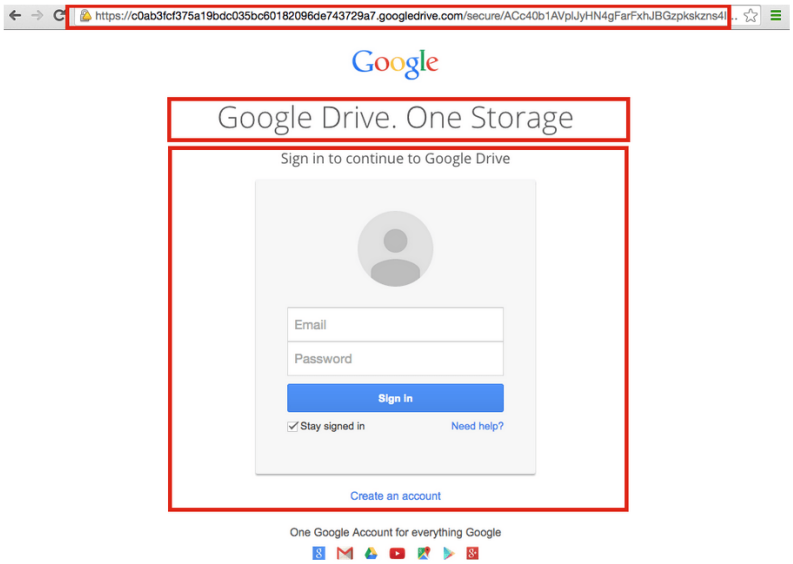
Які мотиви зловмисника надсилати такі листи?

1. Виманити ваші конфіденційні дані.

Злочинець надсилає такий лист з темою «Вас зламали! Швидше змініть пароль» і видає себе за авторитетне джерело – “Google”.



Його мета – щоб ви перейшли за посиланням у листі та нібито підтвердили дані вашого облікового запису, ввівши свій емейл та пароль у відповідні поля. Для цього він створить сайт, який буде майже не відрізнятись від справжнього.



Одержавши ваші секретні дані, злочинець отримає доступ до облікового запису та зможе завантажити цікаву йому інформацію або скористатись ним для наступного етапу атаки (наприклад, на вашу установу).

Додатковим рівнем захисту у цьому випадку буде другий фактор аутентифікації. Адже якщо злодій отримає ваші секретні дані для входу, йому буде необхідно ще мати секретний код, який генерується на вашому телефоні.

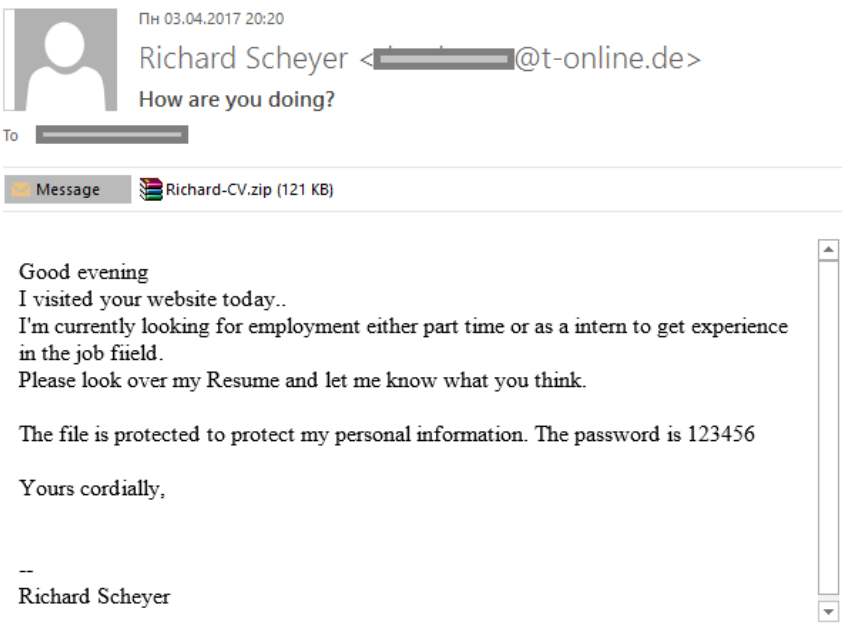
- *Optional «14.02.2018 відбулась фішингова розсилка з електронної адреси otkachenko@me.gov.ua з темою повідомлення «Нарада» та прикріпленими шкідливими файлами – 28.02.docx.exe. При відкритті файлу, запускався шкідливий код Schwarze-Sonne-Remote-Access-Trojan. Цей процес зв'язувався з центром, який віддалено отримував команди від сервера – gordon6.hopto.org."*

2. Зараження системи/мережі організації з метою паралізації всієї системи (шифрування).

Злочинець надсилає листа і видає за себе за авторитетне джерело. Його ціль – щоб ви запустили файл у додатку.

Як тільки ви відкриєте файл, почнеться процес шифрування компьютера з метою подальшого вимагання грошового викупу ключів для відновлення файлів.

Маючи доступ до вашого компьютера, хакери можуть спробувати також отримати доступ до інших комп'ютерних систем, які знаходяться в одній з вами мережі. Вони зацікавлені у заробітку: чим більше шифрують, тим більше вимагають :)


Пн 03.04.2017 20:20

Richard Scheyer <[redacted]@t-online.de>

How are you doing?

To [redacted]

Message Richard-CV.zip (121 KB)

Good evening
I visited your website today..
I'm currently looking for employment either part time or as a intern to get experience in the job fiield.
Please look over my Resume and let me know what you think.

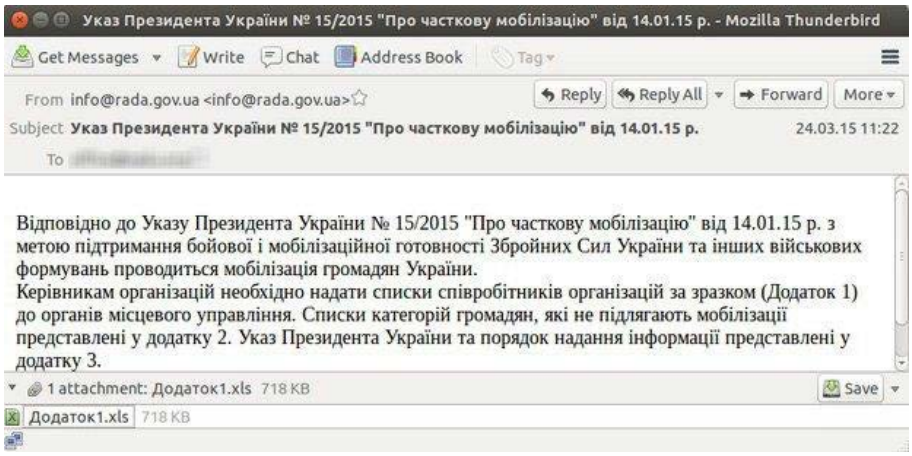
The file is protected to protect my personal information. The password is 123456

Yours cordially,

--
Richard Scheyer

3. Отримання віддаленого доступу до комп'ютера та, як наслідок, мережі.

У 2015 році група хакерів надіслала електронного листа українським енергетичним компаніям з файлом Excel у додатку, видаючи себе за легітимне джерело. При відкритті того файлу, відбувалось зараження комп'ютера та надавало хакерам віддалений доступ для управління системою.



Злочинцям вдалось віддалено вплинути на роботу систем та результатом цієї атаки було:

- «Прикарпаттяобленерго»: вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин.
- «Київобленерго»: відключено 30 вузлових підстанцій, від яких живиться низка стратегічних об'єктів, понад 80 тисяч споживачів були без електрики протягом однієї-трьох годин.

Підсумок:

Кіберзлочинці надсилають фішингові листи з метою:

- Отримання доступу до облікового запису;
- Шифрування вашого комп'ютера;
- Отримання віддаленого доступу.

3. ЯК ВІДРІЗНЯТИ ЛЕГІТИМНІ ЛИСТИ ВІД ФІШИНГОВИХ (INVESTIGATION)

Давайте розберемо, а як же відрізняти легітимні листи від фішингових.

Вам надійшов лист. Ви очікували на нього? Ні?

Проведімо аналіз метаданих.

Аналіз метаданих:

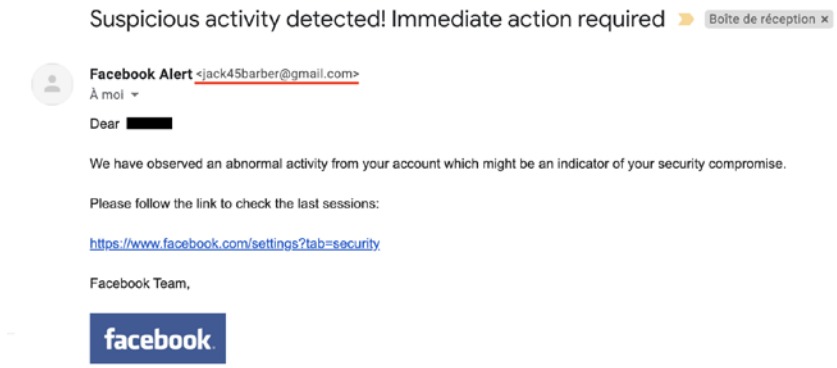
1. Спершу, ми подивимось, хто відправник. Ви знаєте його? Вважайте, ім'я відправника можна поставити будь-яке.

2. Яка тематика повідомлення? Якщо вона викликає якусь квапливість або кличе до швидкої дії, це має бути індикатором, що до листа треба поставитись серйозно та обережно. Приклад: «Вас зламали! Швидше поміняйте пароль».

3. Коли ви відкрили лист, зверніть увагу на правильність написання домену відправника. Кіберзлочинці часто підмінюють літери/символи, щоб замаскуватись під авторитетне джерело. Так, accounts-google.com маскується під accounts.google.com

- *В період президентських виборів у США 2016 року для проведення фішинг-атаки на базі схожих доменів зловмисники використали сайт «accounts-google.com» як клону сайту «accounts.google.com».*

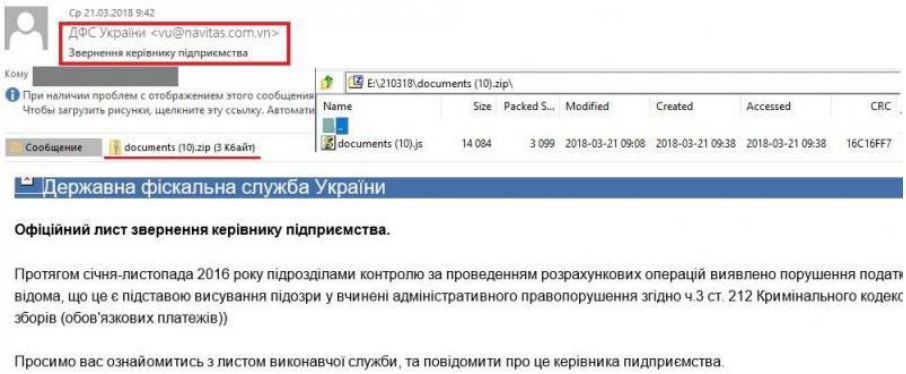
На малюнки знизу, злочинці навіть не маскуються.



Коли ми переконались, що лист надійшов саме з достовірної адреси, ми можемо проаналізувати зміст повідомлення.

Аналіз змісту повідомлення

1. Перше на що варто звернути увагу: чи звертаються до вас на ім'я? Чи використовують загальні фрази «Шановні колеги», «Шановний клієнте» і тд. Злочинець може вказати ваше ім'я, тоді атаку можна вважати підготовленною спеціально під вас.



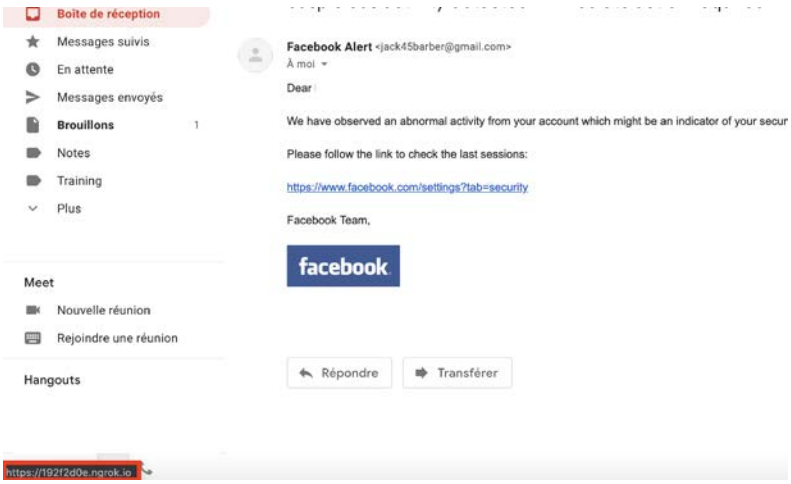
2. Наступний індикатор фішингового листа – мова та наявність граматичних/ орфографічних помилок. Наприклад, "Google" надсилає листи, які стосуються облікового запису, мовою інтерфейсу цього запису. Тобто, якщо у вас інтерфейс українською мовою, а лист прийшов російською, це серйозна причина задуматися.

3. Якщо ви отримуєте файл у додатку та пароль для відкриття його, це є великою підозрою на наявність у ньому шкідливого коду.

Чому? Справа в тому, що у поштових сервісів є свої антивіруси, які сканують файли на наявність вірусів. Злочинці про це також знають, тому використовують функціонал архіваторів (WinRar, ZIP, та інші), щоб зашифрувати вміст файлу паролем.

Таким чином, коли ви отримуєте файл на пошту, поштовий антивірус не може розпізнати шкідливість файлу, оскільки він зашифрований.

4. Далі, подивімось чи є якісь активні посилання у листі? Спробуйте навести мишкою на посилання (не натискаючи) та потримайте декілька секунд. У правому куті, подивіться, куди насправді воно вас веде.



Важливо!!!

- *Посилання такого вигляду accounts.google.com.evilwebsite.pe/EditPasswd також шахрайське, бо адреса має починатися з accounts.google.com/ (тобто, після.com мусить бути /, а не крапка).*

Аналіз додатку

Нарешті, проведімо аналіз додатку до листа.

Подивіться, яке розширення файлу? Кожен тип файлу згаданий нижче, може виконувати код на комп'ютері, тому слід відносити їх до небезпечних розширень:

i. Будь-які виконувані файли: EXE, COM, CMD, BAT, PS1, SWF, JAR, JS, VBS тощо.
ii. Документи MS Office, особливо з макросами: DOC/DOCX/DOCM, XLS/XSLX/XLSM тощо.
iii. PDF-документи: PDF.
iv. Файли векторної графіки з вбудованим кодом: SVG.
v. Як ми вже казали, архіви файлів. Особливо ті, що захищені паролем.

Зауважте!

- *Ми часто користуємось "Microsoft Office" та PDF-файлами, але вони також можуть нести в собі шкідливий код.*

4. ЯК УБЕЗПЕЧИТИ СВОЮ ПОШТОВУ СКРИНЬКУ (РЕКОМЕНДАЦІЇ)

1. Використовувати складний пароль /

Перевірити складність паролю, який буде схожий на ваш (перевірити).

Що таке складний пароль?

Складний пароль – той, який містить в собі літери, символи та цифри і за довжиною не менше 8 символів.

Пароль не повинен містити слів, які можна знайти у словнику.

Приклад поганого паролю:
rockandroll123

Приклад надійного паролю:
T@8l3S0bk4hA7

Але як запам'ятати такі паролі???

- Не передавайте нікому свої паролі

2. Встановити 2-ий фактор аутентифікації посилання на встановлення 2-фактору на всіх платформах

- Google.com
- Facebook.com
- Twitter
- Dropbox
- Apple

Як ми вже бачили, другий фактор аутентифікації використовують для додаткового рівня захисту. Якщо у вашій організації немає 2-го фактору, ви маєте бути більше обачливими.

3. Ніколи не відкривати файли, не переконавшись у їхньому походженні. Використовувати додатковий канал комунікації, аби перевірити, чи дійсно надсилали вам цей лист (наприклад, за допомогою телефону, месенджеру і тд.).

4. Не використовувати службову пошту в особистих цілях.

5. Маєте сумніви щодо походження файлу, використовуйте https://virustotal.com для сканування файлу 50-ма антивірусними програмами.

Note: надсилаючи туди файл, ви надаєте доступ до файлу третім особам.

6. Виходити з сеансу облікового запису.

7. Якщо у листі є скорочені посилання (https://bit.ly/xxxxx ривай їх за допомогою таких сервісів:

http://checkshorturl.com/
http://www.expandurl.net/

5. ЩО РОБИТИ, ЯКЩО ВЖЕ КЛЮНУВ НА ГАЧОК ЗЛОДІЯ?

Якщо перейшов/ла за посиланням у фішинговому листі, тоді:

1. Швидше зміни пароль;
2. Продивись відкриті сесії та закрий ті, які тобі не належать;
3. Повідом про це IT-відділ.

Якщо відкрив файл у додатку і зрозумів/ла, що це був фішинг, тоді:

1. Вимкни комп'ютер;
2. Звернись до відділу IT-технологій.

МОДУЛЬ № 4:

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

МОДУЛЬ №4: ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Шкідливий програмний засіб, шкідливе програмне забезпечення (далі по тексту ШПЗ) – програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Може проявлятися у вигляді коду, скрипту, активного контенту, й іншого програмного забезпечення.

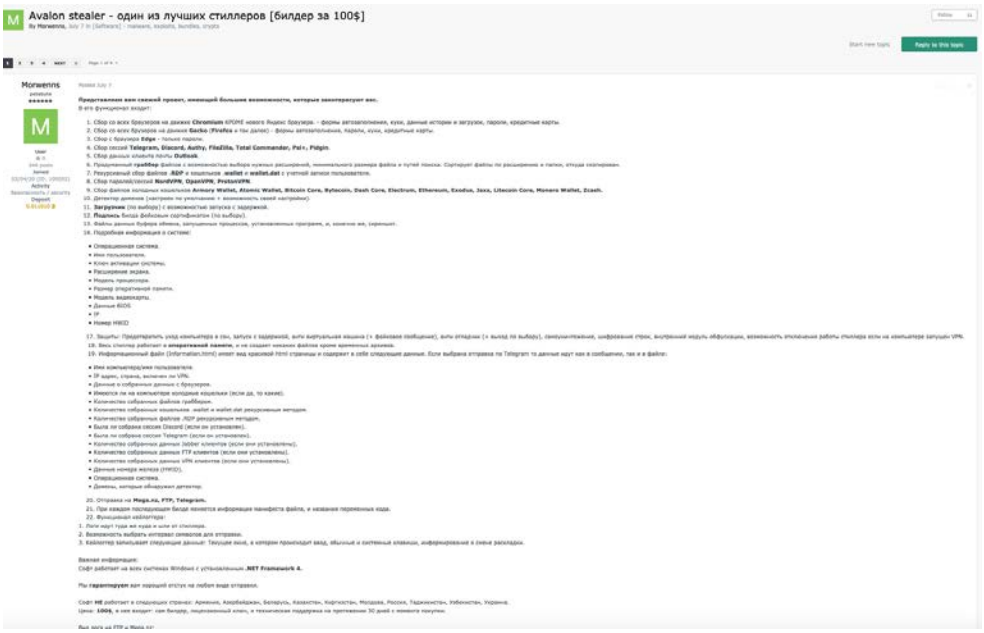
Більша частина шкідливого програмного забезпечення створена з метою викрадення чи блокування персональної інформації та отримання несанкціонованого доступу до неї.

Де береться ШПЗ?

Шкідливе програмне забезпечення може розроблятися зловмисниками «з нуля», а може базуватися на легітимному модифікованому «програмному забезпеченні», зазвичай це троянські програми, які базуються на легальних програмах віддаленого доступу та адміністрування. Прикладом може слугувати "Remote Manipulator System" та "Ammy Admin".

ШПЗ можна купити на спеціалізованих форумах та сайтах в мережі «Інтернет», вартість коливається від декількох десятків доларів то декількох тисяч. Досить часто ШПЗ надається як сервіс (Malware-as-a-service), де клієнт платить місячну/денну/тижневу плату за користування ШПЗ, яке надається «під ключ». Такий підхід значно знижує бар'єр входу та робить ШПЗ доступним для широкого кола осіб.

Нижче наведено приклади реклами вірусів на хакерських форумах.



Avalon stealer - один из лучших стиллеров [билдер за 100$]

By Morwenns, July 7 in [Software] - malware, exploits, bundles, crypts

Start new topic | Reply to this topic

Morwenns

Представляем вам свежий проект, имеющий большие возможности, которые заинтересуют вас.

В его функционал входит:

1. Сбор со всех браузеров на движке **Chromium** КРОМЕ нового Яндекс браузера. - формы автозаполнения, куки, данные истории и загрузок, пароли, кредитные карты.
2. Сбор со всех браузеров на движке **Gecko (Firefox** и тем далее) - формы автозаполнения, пароли, куки, кредитные карты.
3. Сбор с браузера **Edge** - только пароли.
4. Сбор сессий **Telegram, Discord, Authy, FileZilla, Total Commander, Psi+, Pidgin.**
5. Сбор данных клиента почты **Outlook.**
6. Продуманный **граббер** файлов с возможностью выбора нужных расширений, минимального размера файла и путей поиска. Сортирует файлы по расширению и папок, откуда скопирован.
7. Рекурсивный сбор файлов **.RDP** и кошельков **wallet с wallet.dat** с учетной записи пользователя.
8. Сбор паролей/сессий **NordVPN, OpenVPN, ProtonVPN.**
9. Сбор файлов локальных кошельков **Armory Wallet, Atomic Wallet, Bitcoin Core, Bytecoin, Dash Core, Electrum, Ethereum, Exodus, Jaxx, Litecoin Core, Monero Wallet, Zcash.**
10. Детектор дисплеев (настроен по умолчанию + возможность своей настройки).
11. **Загрузчик** (по выбору) с возможностью запуска с задержкой.
12. **Подпись** билда фейковым сертификатом (по выбору).
13. Файлы данных буфера обмена, запущенных процессов, установленных программ, и, конечно же, скриншот.
14. Подробная информация о системе:

- Операционная система.
- Имя пользователя.
- Ключ активации системы.
- Расширение экрана.
- Модель процессора.
- Размер оперативной памяти.
- Модель видеокарты.
- Данные RDDS.
- IP.
- Номер HWID.

17. Защиты: Предотвратить уход компьютера в сон, запуск с задержкой, выпуск виртуальная машина (+ фейковое сообщение), выпуск отладчик (+ выход по выбору), самоудаление, шифрование строк, внутренний модуль обфускации, возможность отключения работы стиллера если на компьютере запущен VPN.
18. Весь стиллер работает в **оперативной памяти**, и не создает никаких файлов кроме временных архивов.
19. Информационный файл (Information.html) имеет вид красивой Html страницы и содержит в себе следующие данные. Если выбрана отправка по Telegram то данные идут как в сообщении, так и в файле:

- Имя компьютера/имя пользователя.
- IP адрес, страна, включен ли VPN.
- Данные о собранных данных с браузеров.
- Имеются ли на компьютере холодные кошельки (если да, то какие).
- Количество собранных файлов граббером.
- Количество собранных кошельков .wallet и wallet.dat рекурсивным методом.
- Количество собранных файлов .RDP рекурсивным методом.
- Была ли собрана сессия Discord (если он установлен).
- Была ли собрана сессия Telegram (если он установлен).
- Количество собранных данных Jabber клиентов (если они установлены).
- Количество собранных данных FTP клиентов (если они установлены).
- Количество собранных данных VPN клиентов (если они установлены).
- Данные номера жертвы (HWID).
- Операционная система.
- Домены, которые обнаружил детектор.

20. Отправка на **Mega.nz, FTP, Telegram.**
21. При каждом последующем билде меняется информация манифеста файла, и названия переменных кода.
22. Функциональ кейлоггера:

1. Логи идут туда же куда и сам от стиллера.
2. Возможность выбрать интервал сливалов для отправки.
3. Кейлоггер записывает следующие данные: Текущее окно, в котором производит ввод, обычные и системные клавиши, информирование о смене раскладки.

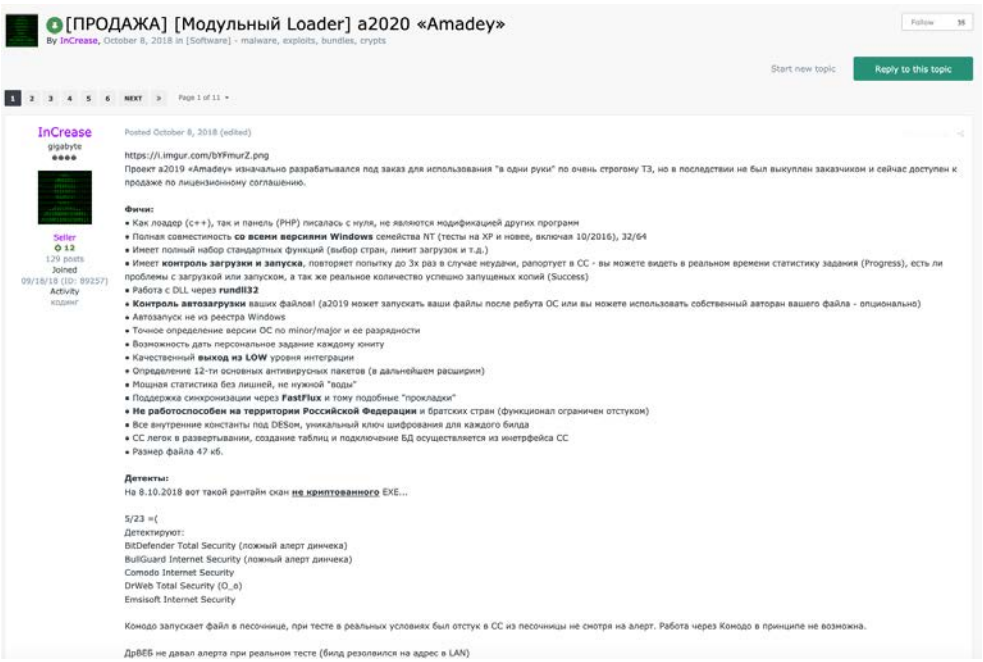
Важная информация:

Софт работает на всех системах Windows с установленным **.NET Framework 4.**

Мы **гарантируем** вам хороший отступ на любом виде отправки.

Софт **НЕ** работает в следующих странах: Армения, Азербайджан, Беларусь, Казахстан, Киргизстан, Молдова, Россия, Таджикистан, Узбекистан, Украина.

Цена: **100$**, в нее входит: сам билдер, лицензионный ключ, и техническая поддержка на протяжении 30 дней с момента покупки.



[ПРОДАЖА] [Модульный Loader] a2020 «Amadey»

By InCrease, October 8, 2018 in [Software] - malware, exploits, bundles, crypts

Start new topic | Reply to this topic

InCrease

gigabyte

Seller

12

129 posts

Joined

09/18/18 (ID: 89257)

Activity

кодинг

Posted October 8, 2018 (edited)

https://i.imgur.com/bYFmurZ.png

Проект a2019 «Amadey» изначально разрабатывался под заказ для использования "в одни руки" по очень строгому ТЗ, но в последствии не был выкуплен заказчиком и сейчас доступен к продаже по лицензионному соглашению.

Фичи:

- Как лоадер (c++), так и панель (PHP) писалась с нуля, не являются модификацией других программ
- Полная совместимость **со всеми версиями Windows** семейства NT (тесты на XP и новее, включая 10/2016), 32/64
- Имеет полный набор стандартных функций (выбор стран, лимит загрузок и т.д.)
- Имеет **контроль загрузки и запуска**, повторяет попытку до 3х раз в случае неудачи, рапортует в CC - вы можете видеть в реальном времени статистику задания (Progress), есть ли проблемы с загрузкой или запуском, а так же реальное количество успешно запущеных копий (Success)
- Работа с DLL через **rundll32**
- **Контроль автозагрузки** ваших файлов! (a2019 может запускать ваши файлы после ребута ОС или вы можете использовать собственный авторан вашего файла - опционально)
- Автозапуск не из реестра Windows
- Точное определение версии ОС по minor/major и ее разрядности
- Возможность дать персональное задание каждому юниту
- Качественный **выход из LOW** уровня интеграции
- Определение 12-ти основных антивирусных пакетов (в дальнейшем расширим)
- Мощная статистика без лишней, не нужной "воды"
- Поддержка синхронизации через **FastFlux** и тому подобные "прокладки"
- **Не работоспособен на территории Российской Федерации** и братских стран (функционал ограничен отстуком)
- Все внутренние константы под DESом, уникальный ключ шифрования для каждого билда
- CC легок в развертывании, создание таблиц и подключение БД осуществляется из инетрфейса CC
- Размер файла 47 кб.

Детекты:

На 8.10.2018 вот такой рантайм скан **не криптованного** EXE...

5/23 =(

Детектируют:

BitDefender Total Security (ложный алерт динчека)

BullGuard Internet Security (ложный алерт динчека)

Comodo Internet Security

DrWeb Total Security (O_o)

Emsisoft Internet Security

Комодо запускает файл в песочнице, при тесте в реальных условиях был отстук в CC из песочницы не смотря на алерт. Работа через Комодо в принципе не возможна.

ДрВЕБ не давал алерта при реальном тесте (билд резолвился на адрес в LAN)

Приклади масових вірусних атак:

https://uk.wikipedia.org/wiki/Кібератака_на_енергетичні_компанії_України
https://ru.wikipedia.org/wiki/Хакерские_атаки_на_Украину_(2017)

[показ новин у вигляді слайдів чи нарізок відео і голос за кадром розповідає про атаки що вище, і спричинені наслідки]

1. ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

1.1. Існує декілька найпоширеніших шляхів розповсюдження ШПЗ, серед них безумовним фаворитом є спам.

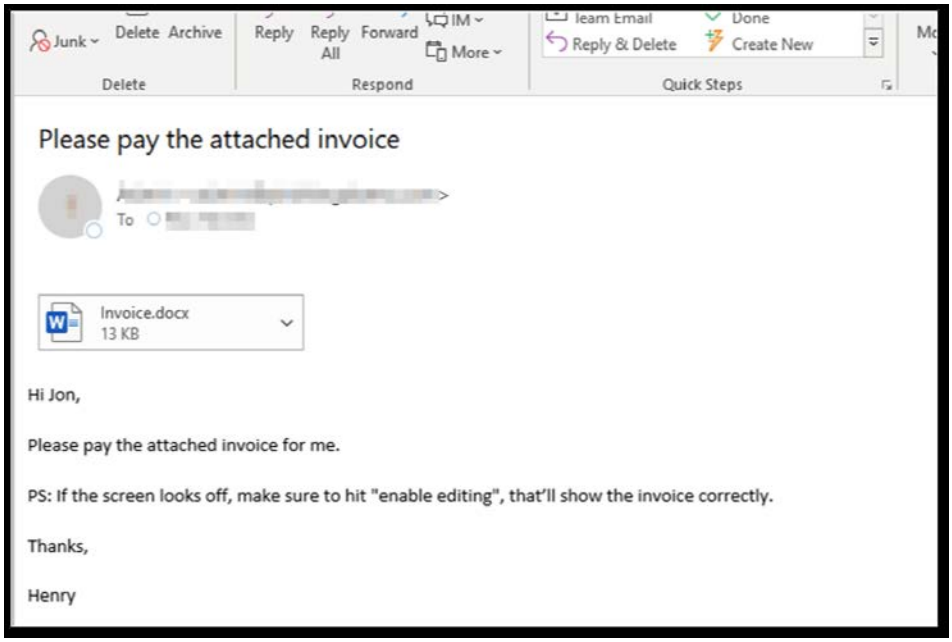
Звичайний спам – надсилається масово широкому колу осіб. Хакери можуть надсилати спам, атакуючи певні галузі, наприклад страхові компанії, медичні установи, державні структури; або надіслати спам користувачу певної країни. Спам-бази зазвичай купують на хакерських форумах.

Таргетовані або цільові спам-кампанії, це коли хакер надсилає спеціально створений лист, адресований конкретній особі або організації. Це більш складний тип атаки, оскільки таргетовані спам-кампанії, передбачають попереднє вивчення майбутньої жертви, наприклад, її активності в соціальних мережах, родинних зв'язків, вподобань, хобі, життєвих проблеми тощо. Ця інформація дозволяє хакеру якнайточніше сформувати лист, щоб змусити жертву запустити вірус.

> *Таргетована або цільова атака – це вид кібератаки, спрямований на конкретну ціль, це може бути компанія, державна структура чи користувач. Таргетована атака відрізняється від масової тим, що перед її здійсненням атакуючий детально вивчає свою ціль, збирає про неї всі наявні дані та, виходячи з цього, планує та організовує атаку.*

Хакери надсилають ШПЗ у вигляді вкладення до емейлу, це може бути файл MS Word/Excel, PDF, PNG тощо із спеціальним вставленним скриптом, який після його активізації завантажить ШПЗ із віддаленого серверу та запустить на комп'ютері жертви.

Іншим способом є надсилання шкідливого файлу із «фейковим або так званим подвійним розширенням». У такому випадку хакери змінюють розширення файлу та змінюють іконку файлу на відповідну розширенню. Це створює враження, що файл є безпечним та може бути відкритий у комп'ютері. Наприклад, файл note.txt.exe насправді є виконуваним файлом, а не текстовим, хоча якщо у користувача вимкнено функцію показувати розширення файлів, у нього складеться враження, що він відкриває текстовий файл і таким чином запустить вірус.



Щоб увімкнути функцію «Показувати розширення файлів»:*

- Натисніть кнопку «Пуск» і виберіть пункт меню «Мій комп'ютер».
- Далі в меню оберіть пункт «Сервіс», потім пункт «Властивості папки».
- У вікні «Властивості папки», виберіть вкладку «Вигляд».
- Знайдіть пункт «Приховувати розширення для зареєстрованих типів файлів» і зніміть з нього галочку.

Для того, щоб змусити жертву відкрити вкладений шкідливий файл, хакери застосовують засоби соціальної інженерії.

* може дещо відрізнятися залежно від версії операційно системи.

Як альтернатива, злочинці можуть вставляти посилання на завантаження ШПЗ напряму в емейл та маскувати його під виглядом легітимної програми чи додатку. На зображеннях, що нижче, Ви можете бачити, приклади фішингових листів, які використовували тему світової пандемії коронавірусу 2020 для розповсюдження ШПЗ.

Фішинг – *це вид онлайн шахрайства, який базується на методах соціальної інженерії та має на меті, шляхом обману, змусити користувача здійснити дії, які б він не здійснив у звичних умовах, наприклад, розкрити свої персональні дані, завантажити, встановити чи запустити шкідливе програмне забезпечення. Фішинг може бути здійснений у різних формах – електронні листи, надіслані нібито від імені легальних компаній, фейкові вебсайти, дзвінки нібито співробітників банку, тощо.*

Coronavirus - Recommendations to prevent infection spread

World Health Organization

Coronavirus Cases:	Deaths:	Recovered:
1,203,428	64,754	246,803

Dear

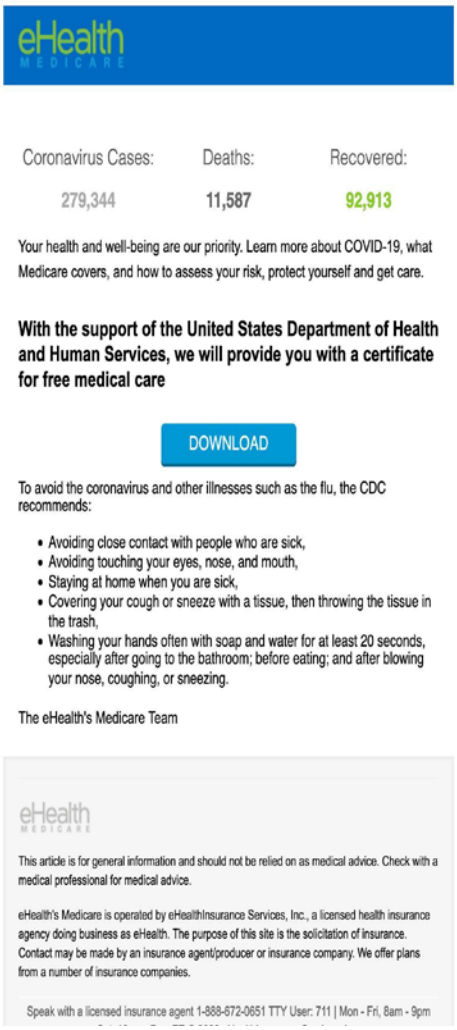
Common signs of infection include respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. In more severe cases, infection can cause pneumonia, severe acute respiratory syndrome, kidney failure and even death.

Recommendations to prevent infection spread include regular hand washing, covering mouth and nose when coughing and sneezing, thoroughly cooking meat and eggs. Avoid close contact with anyone showing symptoms of respiratory illness such as coughing and sneezing.

If you want to know how many people are infected in your city, follow the link and download our application

Sincerely,
Department of Public Health
© 2020 WHO

This is an automatically generated message.



eHealth
MEDICARE

Coronavirus Cases:	Deaths:	Recovered:
279,344	11,587	92,913

Your health and well-being are our priority. Learn more about COVID-19, what Medicare covers, and how to assess your risk, protect yourself and get care.

With the support of the United States Department of Health and Human Services, we will provide you with a certificate for free medical care

DOWNLOAD

To avoid the coronavirus and other illnesses such as the flu, the CDC recommends:

- Avoiding close contact with people who are sick,
- Avoiding touching your eyes, nose, and mouth,
- Staying at home when you are sick,
- Covering your cough or sneeze with a tissue, then throwing the tissue in the trash,
- Washing your hands often with soap and water for at least 20 seconds, especially after going to the bathroom; before eating; and after blowing your nose, coughing, or sneezing.

The eHealth's Medicare Team

eHealth
MEDICARE

This article is for general information and should not be relied on as medical advice. Check with a medical professional for medical advice.

eHealth's Medicare is operated by eHealthInsurance Services, Inc., a licensed health insurance agency doing business as eHealth. The purpose of this site is the solicitation of insurance. Contact may be made by an insurance agent/producer or insurance company. We offer plans from a number of insurance companies.

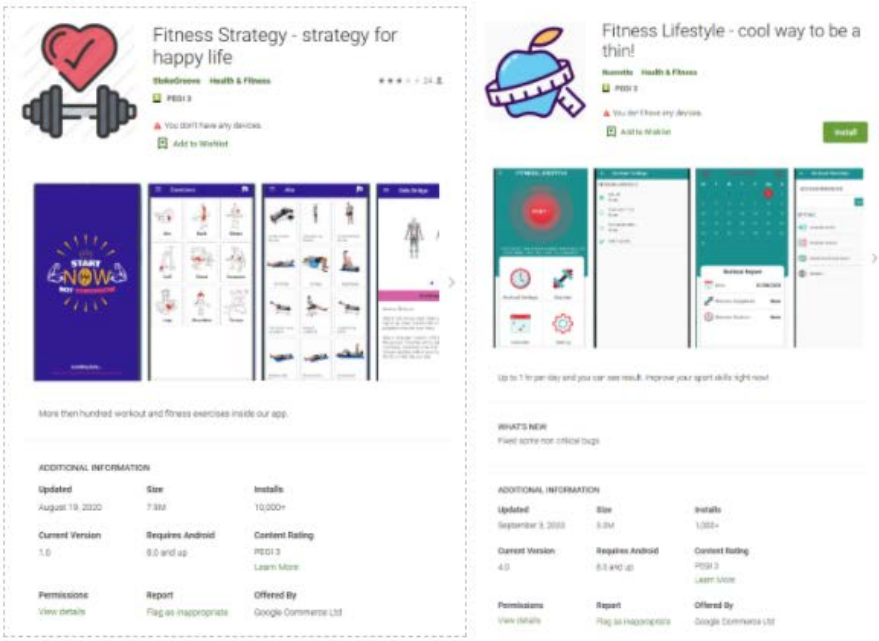
Speak with a licensed insurance agent 1-888-672-0651 TTY User: 711 | Mon - Fri, 8am - 9pm

2.2. Іншим не менш поширеним способом розповсюдження ШПЗ є розповсюдження так званих для комерційного програмного забезпечення або самих примірників «зламаного» комерційного програмного забезпечення, яке «не потребує ліцензії».

> *«Кряк» (від англійського "crack"), це програма, яка генерує код активації для комерційного програмного забезпечення чи змінює систему перевірки ліцензійності комерційного програмного забезпечення і тим самим порушує авторські права виробника.*

У такому випадку, хакери додають шкідливий програмний код в модифіковане комерційне програмне забезпечення. Нічого не підозрюючи, користувач встановлює таку програму і разом з нею вірус, який отримує доступ до системних файлів. На скріншоті, що нижче, Ви можете побачити реальний приклад розповсюдження програми вимагача (ransomware) під виглядом так званої програми активатора для "Windows".

Різновидом цього способу є поширення ШПЗ під виглядом "freeware" программ. Це, як правило, так звані «корисні» програми, такі як ліхтарики для мобільних телефонів, калькулятори, конвертери валют тощо. Найбільш поширеними вони є для мобільних пристроїв. На малюнках, що нижче зображено дві програми фітнес-тренери, які насправді встановлювали на мобільний телефон банківський троян.

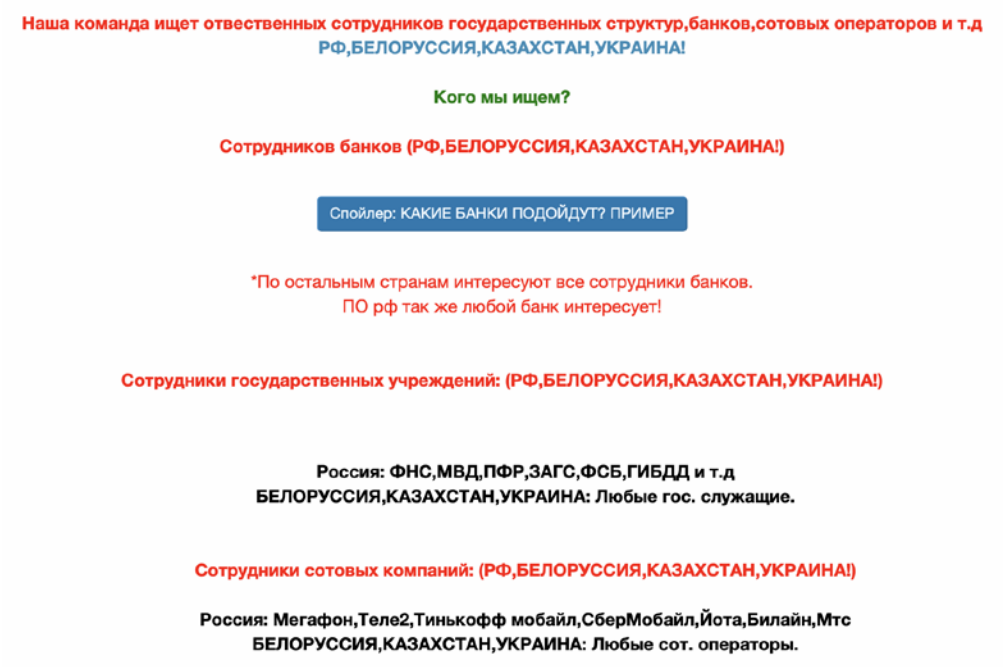


Рекомендації, як визначити, що програма підозріла і може завдати шкоди Вашому пристрою:

- Подивитися рейтинг програми та почитати відгуки.
- Подивитися інформацію, до яких функцій операційної системи програма отримує доступ або просить надати доступ. Очевидно, що програмі ліхтарик, не потрібний доступ до ваших текстових повідомлень, камери, мікрофону чи фотографій, щоб ефективно працювати.
- Подивитися інформацію щодо розробника. Чи це відома фірма, чи невідомий розробник? Чи існує взагалі якась інформація щодо розробника у відкритих джерелах? Чи завантажив розробник в “Google Play Market” інші програми, скільки, який їх рейтинг? Чи є у розробника власний сайт тощо.
- Не встановлюйте програми із низьким рейтингом та малою кількістю завантажень.
- Пам’ятайте, що краще заплатити кілька сотень гривень за ліцензійну програму, ніж потім втратити тисячі із власного банківського рахунку.

1.3. Таргетовані атаки із використанням «нетрадиційних методів». Сюди можна віднести «випадково загублені флешки», фізичний доступ хакеру до комп'ютера, складні прийоми соціальної інженерії, коли телефонують користувачеві та просять встановити ту чи іншу програму, наприклад, під виглядом співробітників банку. Окремої уваги заслуговує загроза від інсайдерів, які вербуються хакерами для встановлення вірусів, відключення антивірусів та фаєрволів.

https://www.zdnet.com/article/elon-musk-confirms-russian-hacking-plot-targeted-tesla-factory/



2. ВИДИ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Є різні підходи до класифікації шкідливого програмного забезпечення, залежно від цілей ШПЗ, методів розповсюдження, векторів атаки, ітд. Ми даємо класифікацію, виходячи з цілей використання ШПЗ та його функціоналу.

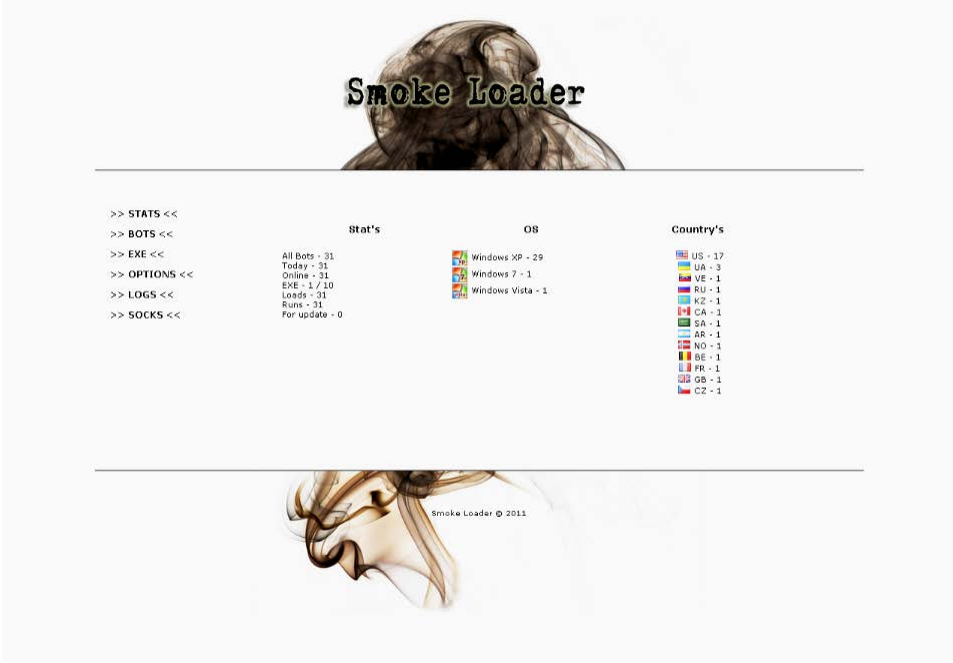
- *Слід зазначити, що на практиці ШПЗ зазвичай є модульним та включає в себе одночасно декілька функцій наведених нижче. Наприклад, Agent Tesla – це шкідливе програмне забезпечення (далі – ШПЗ), яке виконує функції кейлоггера (keylogger), викрадача інформації (stealer) та є вдосконаленим трояном віддаленого доступу (RAT).*

Залежно від цілей та функціоналу можна виділити такі види ШПЗ:

2.1. Завантажувач (дропер/лоадер) (Eng. malware loaders or droppers)

Функцією дропера є завантаження та запуск головного модуля ШПЗ. Лоадер, як правило, мають малий розмір, в декілька десятків або сотень кілобайт, та мінімальний функціонал – завантаження та запуск «головного модуля» ШПЗ. Це надає дроперам додаткові переваги уникати антивірусних програм. На відміну від іншого ШПЗ, це дозволяє їм, як правило, безперешкодно проходити повз встановлені антивірусні системи, прописувати свій код в системі. Після потрапляння в систему, дропер за командою або автоматично завантажує головний модуль або "second stage payload." Це може бути все, що завгодно: інфостілер, ransomware, майнера тощо.

Дропер може бути у вигляді простого скрипту, який завантажує інше ШПЗ за заздалегідь визначеним посиланням (наприклад JS loader) або мати більш складний функціонал та систему управління (control panel), розташовану на віддаленому сервері.

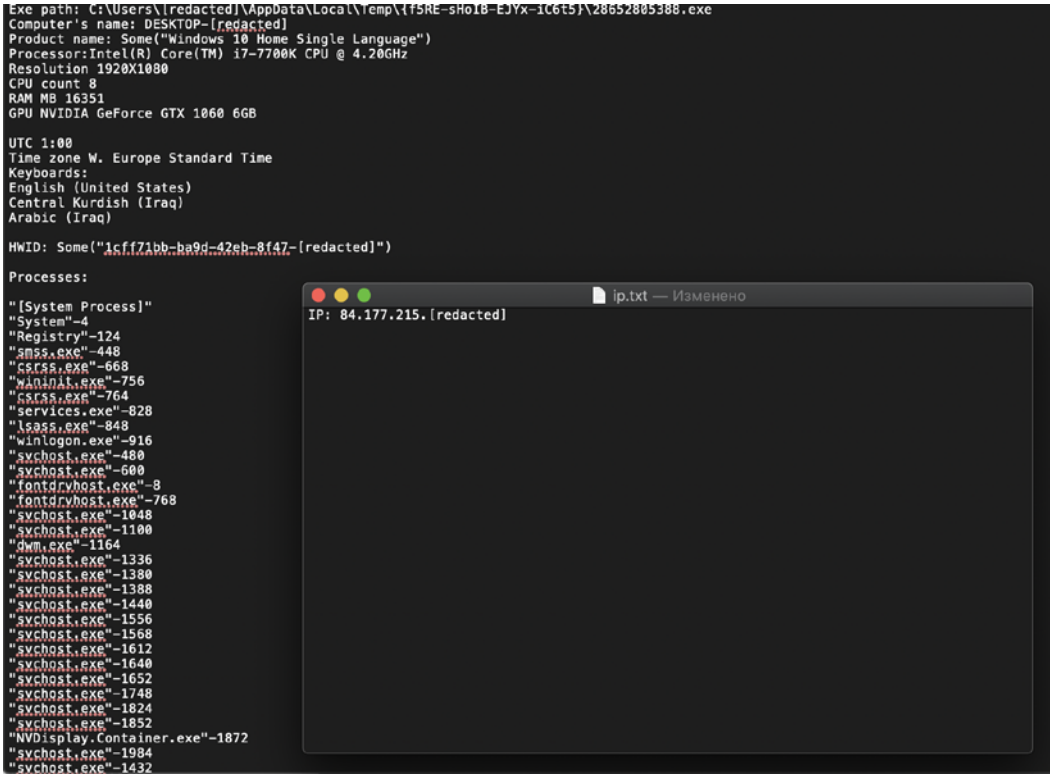


2.2. ***Викрадач інформації «Інфостілер або стілер» (Eng. Information stealers)*** – це вид шкідливого програмного забезпечення, створеного з метою викрадення персональних даних користувачів, у тому числі логінів та паролів, які зберігаються в інтернет-браузерах, месенджерах та різноманітних мережевих клієнтах.

Інфостілери викрадають інформацію про паролі та логіни користувачів, а також додаткову інформацію про систему, яка допоможе атакуючому використати та монетизувати викраденні дані (Тип операційної системи, IP-адресу жертви, cookie-файли тощо).

Приклад логу стілера:

Имя	Дата изменения	Тип	Размер
Browsers	2018.08.23. 3:31	Папка с файлами	
Coins	2018.08.23. 3:31	Папка с файлами	
Skype	2018.08.23. 3:31	Папка с файлами	
Telegram	2018.08.23. 3:31	Папка с файлами	
CookieList	2018.08.23. 3:31	Текстовый докум	20 КБ
ip	2018.08.23. 3:31	Текстовый докум	1 КБ
PasswordsList	2018.08.23. 3:31	Текстовый докум	55 КБ
scr	2018.08.23. 3:31	Файл "JPG"	133 КБ
System	2018.08.23. 3:31	Текстовый докум	33 КБ



```
Browser: Google_Chrome_User Data_Default
Url: https://login.live.com/login.srf
User: he[redacted]@outlook.com
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://login.live.com/login.srf
User: [redacted]@hotmail.com
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://www.dropbox.com/dropins/login
User: [redacted]@gmail.com
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://flixpress.com/Register/tabid/79/Default.aspx
User: [redacted]
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://www.instagram.com/
User: [redacted]
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://ottplayer.es/account/registration
User: [redacted]@gmail.com
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://www.storyblocks.com/join/aff-unlimited-monthly
User: [redacted]@yahoo.com
Password: [redacted]

Browser: Google_Chrome_User Data_Default
Url: https://www.instagram.com/accounts/login/
User: [redacted]@gmail.com
Password: [redacted]@@

Browser: Google_Chrome_User Data_Default
Url: https://login.yahoo.com/m
User: [redacted]@yahoo.com
Password: [redacted]
```

Викрадена інформація надсилається до C&C, чим може бути окрема вебпанель, телеграм-бот, e-mail.

Інфостілери не забезпечують віддаленого доступу до інфікованої системи, але виступають ефективним інструментом для збору конфіденційної інформації та первинного вектору атаки на комп'ютерні мережі.

Одним із підвидів стілерів є «кліпери» (clipper) – цей вид ШПЗ створений для викрадення криптовалют. Шкідливий програмний код активізується в момент, коли жертва переказує криптовалюту. Clipper «на льоту» в оперативній пам'яті комп'ютера підмінює номер гаманця адресата на гаманець хакера, і, нічого не підозрюючи, жертва переказує кошти, які потрапляють на гаманець хакера.

2.3. Keylogger "кейлогер" (англ. key** (stroke)* – клавіша, англ. ***logger – реєструючий пристрій) – це програмний продукт або апаратний пристрій, що реєструє кожне натискання клавіш клавіатури комп'ютера. На даний момент функціонал кейлогерів значно розширився і вони можуть перехоплювати інформацію з вікон програм, кліків миші, буферу обміну; робити фотознімки екрану і активних вікон; моніторити файлову активність тощо; перехоплювати дані з монітору, вебкамери, принтера тощо.

Апаратний кейлогер, встановлюється між клавіатурою та комп'ютером або в саму клавіатуру.

2.4. «JS-сніфери» – шкідливі програмні скрипти, які «вставляються» в програмний код зламаних вебсайтів та використовуються для викрадення даних платіжних карток. JS-сніфер – це зазвичай декілька рядків програмного коду, який зловмисники встановлюють на сторінках із формами онлайн-оплати і які активуються, коли користувач вводить дані платіжних карток.

Ризик «JS сніферів» у тому, що кінцевий користувач практично не має інструментів захисту, адже уражається інфраструктура з боку вебсайту (серверу). Індікатором того, що ви стали жертвою «JS-сніфера» може бути «підозріла» активність за платіжними картками.

2.5. Троянські програми віддаленого доступу RAT (remote access trojans)

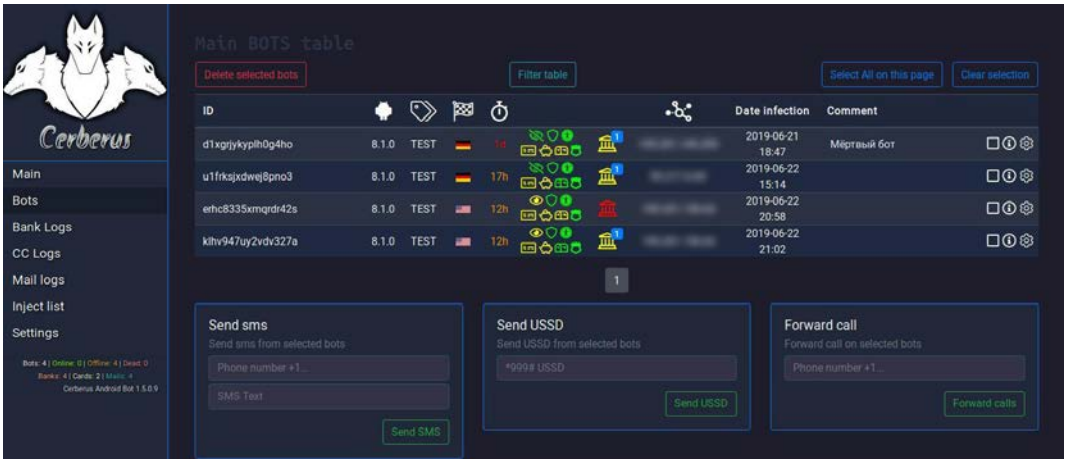
Троянські програма або троян забезпечує хакеру віддалений доступ до інфікованої системи. В такому випадку атакуючий може отримати контроль над усіма файлами, завантажувати файли, модифікувати їх, виконувати від імені користувача дії на комп'ютері, переглядати веббраузер, користуватися поштовим клієнтом та іншим програмним забезпеченням. Троянські програми часто працюють на базі легітимних протоколів операційної системи RDP, VNC і часто розроблені на базі легітимного програмного забезпечення для віддаленого адміністрування комп'ютерів. Це часто призводить до того, що антивірусні програми трактують їх як офіційне програмне забезпечення.

2.6. Банківські трояни (banking trojans)

Вид шкідливого програмного забезпечення, створений з метою викрадення коштів із банківських рахунків. Банківські трояни, це комплексне, багатофункціональне ШПЗ, яке поєднує в собі функції кейлогера та стілера, троянської програми. Після потрапляння на комп'ютер жертви, банківський троян моніторить активність користувача та збирає персональні дані. Як тільки користувач логіниться в особистий кабінет онлайн-банкінгу, ШПЗ перехоплює сесію веббраузера, застосовуючи man-in-the-middle атаку. За такого сценарію, банківський троян відображає точну копію банківської сторінки і, нічого непідозрюючи, користувач вводить свої персональні

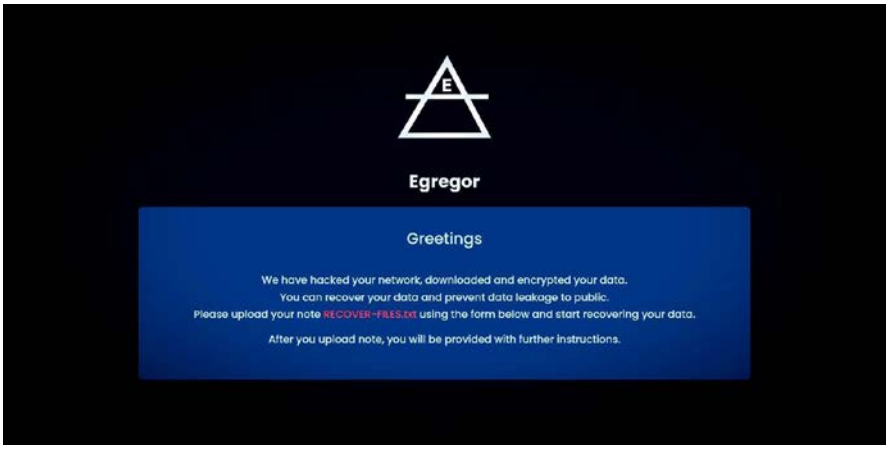
дані (логін, пароль, код 2FA авторизації), які передаються на север хакера. Далі хакер, використовує викрадену сесію для переказу коштів на підконтрольний йому рахунок. Користувач, як правило, бачить у своєму браузері повідомлення, що зв'язок із банком на даний момент неможливий чи, навпаки, йому відображається повідомлення, що браузер намагається встановити з'єднання із сервером банку.

Банківські трояни набули популярності із мобільними технологіями і найбільш ураженими є мобільні прилади під керуванням операційної системи Андроїд.



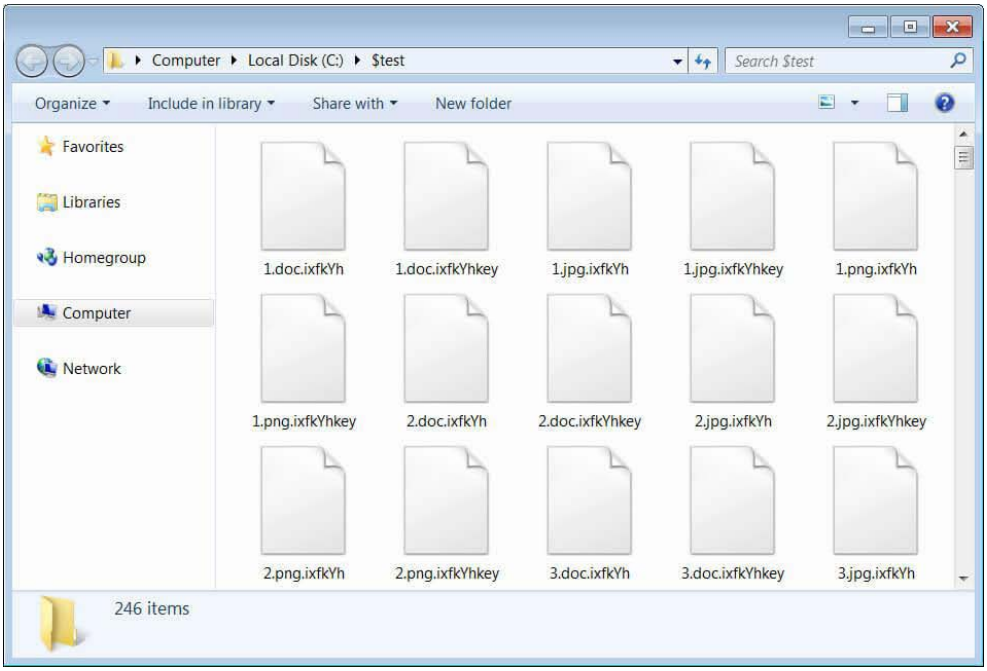
2.7. Ransomware (програма-вимагач, програма-шантажист) – це тип шкідливої програми, яка після потрапляння на комп'ютер шифрує файли та злочинці вимагають викуп за їх розшифрування.

На малюнках, що нижче, зображено повідомлення з вимогою сплатити викуп за відновлення доступу до файлів.



Ransomware шифрує файли із використанням алгоритмів шифрування, які, як правило, не піддаються зламу та розшифруванню, якщо не знати ключів шифрування. Ransomware, як правило, шифрує незначну частину файлу, що значно підвищує швидкість шифрування та все одно робить файли непридатними для використання.

На малюнку, що нижче, зображено файли вражені ransomware:

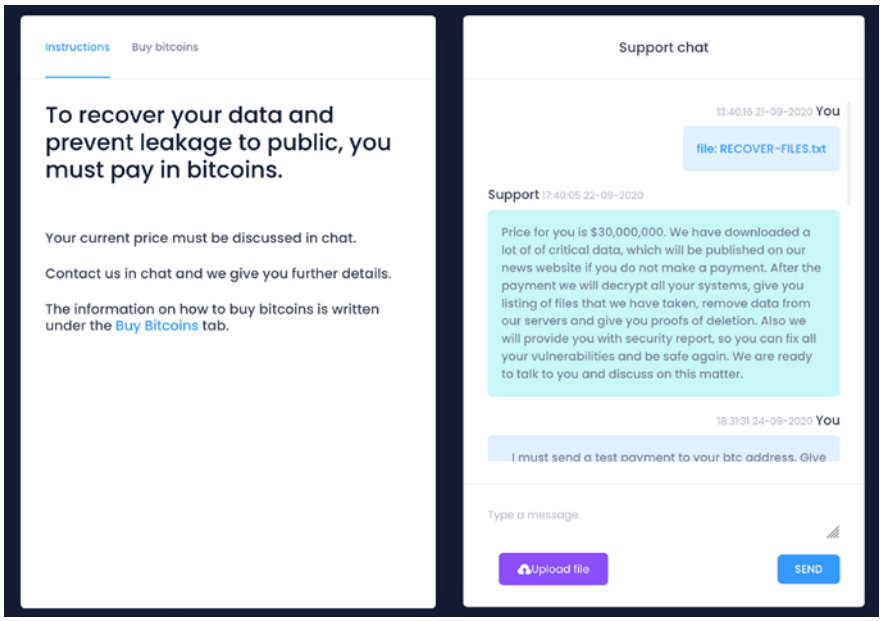


В останні роки ***ransomware*** – один із найпривабливіших видів кіберзлочинів. Суми викупів коливаються від декількох сотень доларів до десятків мільйонів.

Woman dies during a ransomware attack on a German hospital
https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity

SoftServe подверглась атаке хакеров
https://ain.ua/2020/09/01/softserve-haknuli/

Hackers are holding foreign exchange company Travelex to ransom after a cyber-attack forced the firm to turn off all computer systems and resort to using pen and paper.
https://www.bbc.com/news/business-51017852



Ransomware, в основному, атакує корпоративний сектор, деякі групи (Dharma-family) здійснюють атаки на звичайних юзерів.

2.8. Майнери (miners) – ШПЗ, яке без відома жертви використовує потужності її комп'ютера для майнингу криптовалюти. Майнери активізуються лише тоді, коли вражена система не завантажена іншими ресурсозатратним завданнями, щоб не викликати підозру користувача.

Майнери, як правило, одні із самих безобідних видів ШПЗ, вражають всі види операційних систем, включаючи "Linux". Одним із індикаторів, що ви стали жертвою майнера є «безпідставне» навантаження на систему, особливо в моменти, коли ніякі «трудомісткі» програми не були запущені.

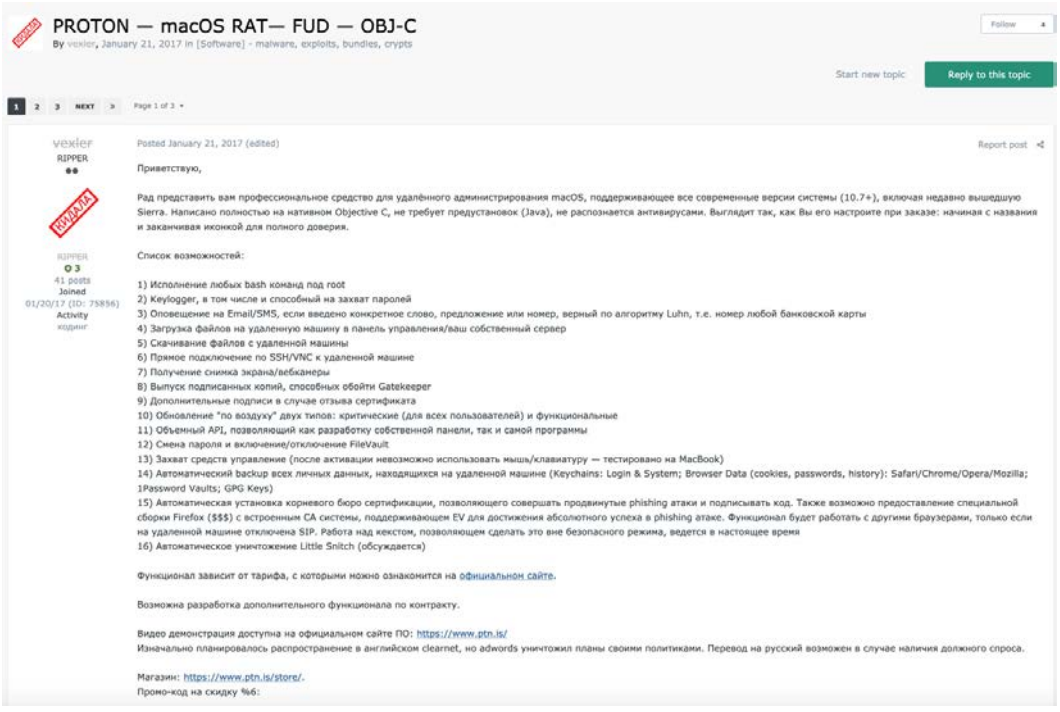
2.9. Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення (Destructive malware) – головною ціллю ШПЗ є знищення важливих та критичних файлів, щоб унеможливити доступ до операційної системи. Файли, як правило, стираються і дисковий простір перезаписується декілька разів, щоб унеможливити відновлення файлів. Атаки з використанням ***destructive malware*** порівняно рідкі, мають або «хуліганський» підтекст, або є частиною **"state sponsored"**-атак на критичні об'єкти інфраструктури. Доволі

часто destructive malware використовується, щоб приховати сліди інших атак. Одним із прикладів ***destructive malware***-атаки є розповсюдження вірусу-шифрувальника Petya, який, хоч і позиціонував себе як **ransomware**, фактично був ***destructive malware.***

2.10. Рекламне шкідливе програмне забезпечення (Adware) – ШПЗ основною ціллю, якого є показ користувачеві реклами, а також збору інформації маркетингового характеру про користувача.

Практично всі згадані вище види ШПЗ створені як для персональних комп'ютерів під керуванням операційної системи "Windows", в тому числі серверні системи, так і мобільні операційні системи, особливо "Android".

Існує загальне думка, що вірусів для "Linux" та "MacOS" не існує, – це помилкове враження, ці операційні системи також вразливі для ШПЗ, хоча його кількість порівняно із ШПЗ для Windows є значно меншою.



3. ОЗНАКИ ТОГО, ЩО Я БУВ ІНФІКОВАНИЙ ШПЗ

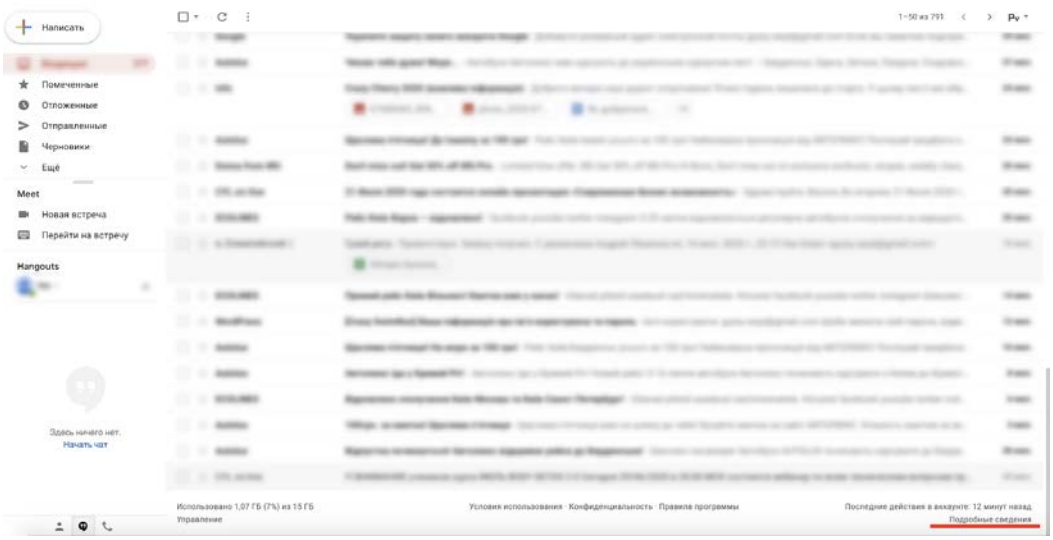
Поміж загальних ознак, таких як повільна робота комп'ютера (мобільного пристрою), поява рекламних повідомлень, постійні безпричинні перезавантаження, відключений антивірус, значна мережева активність, брак системних ресурсів, поява на робочому столі чи екрані смартфону невідомих іконок або іконок програм, які ви не встановлювали, тощо; можна виділити декілька специфічних ознак:

3.1. Підозріла активність акаунтів у соціальних мережах, поштових акаунтів тощо.

- вам прийшло повідомлення, що хтось намагався залогінитися у Ваш Facebook, Twitter, Gmail, тощо.
- ви помітили IP-адреси, з яких не здійснювали доступ до своїх акаунтів, чи підозрілі прилади, які здійснювали доступ.
- Ви помітили емейли, дописи, пости, фото, які особисто не додавали або не надсилали.

За таких обставин, Ви найімовірніше стали жертвою інфостілера, кейлоггера, трояна віддаленого доступу.

Gmail:



Действия пользователя в этом аккаунте

Эта функция позволяет узнать о последних действиях в данном аккаунте электронной почты, а также обо всех сеансах, активных в данный момент. Подробнее...

Скорее всего, этот аккаунт больше нигде не открыт. Однако могут присутствовать незавершенные сеансы.

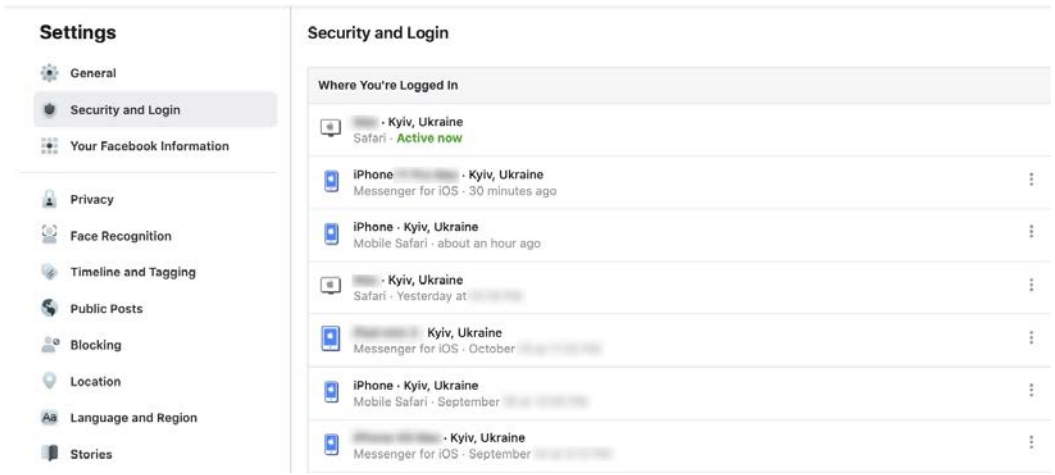
Подробности смотрите на странице Проверка безопасности

Последние действия:

Тип доступа [?] (Браузер, мобильное устройство, POP3 и т. д.)	**Местоположение (IP-адрес) [?]**	**Дата и время** (отображается в вашем часовом поясе)
Браузер (Safari) Скрыть *"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15,gzip(gfe),gzip(gfe)"*	* Украина (46.211)	22:36 (3 мин. назад)
Браузер (Safari) Показать подробную информацию	Украина (46.211.)	22:20 (19 мин. назад)
Браузер (Safari) Показать подробную информацию	Украина (46.211.)	20 окт. (1 день назад)
Браузер (Safari) Показать подробную информацию	Украина (46.211)	20 окт. (1 день назад)
Браузер (Safari) Показать подробную информацию	Украина (46.211.)	20 окт. (1 день назад)
Браузер (Safari) Показать подробную информацию	Украина (46.211.)	20 окт. (1 день назад)
Браузер (Safari) Показать подробную информацию	Украина (46.211.)	20 окт. (1 день назад)
Браузер (Safari) Показать подробную информацию	* Украина (91.227.)	13 окт.
Браузер (Safari) Показать подробную информацию	* Украина (91.227.)	13 окт.
Браузер (Safari) Показать подробную информацию	* Украина (91.227.)	12 окт.

* указывает на действия в текущем сеансе.

IP-адрес этого компьютера: 46.211. (Украина)



Settings

General
Security and Login
Your Facebook Information
Privacy
Face Recognition
Timeline and Tagging
Public Posts
Blocking
Location
Language and Region
Stories

Security and Login

Where You're Logged In

· Kyiv, Ukraine
Safari · Active now

iPhone · Kyiv, Ukraine
Messenger for iOS · 30 minutes ago

iPhone · Kyiv, Ukraine
Mobile Safari · about an hour ago

· Kyiv, Ukraine
Safari · Yesterday at

Kyiv, Ukraine
Messenger for iOS · October

iPhone · Kyiv, Ukraine
Mobile Safari · September

· Kyiv, Ukraine
Messenger for iOS · September

Дії:

- Негайно змінити усі паролі, встановити двохфакторну аутентифікацію.
- Перевірити систему антивірусом чи іншою програмою із виявлення ШПЗ.
- Звернутися по допомогу до спеціалістів з інформаційної безпеки (IT-департамент, приватні фірми).

3.2. Вам надійшло повідомлення від Вашого банку про списання, або спробу списання коштів.

За таких обставин, Ви найімовірніше стали жертвою JS Sniffer або банківського трояна, кейлогера, стілера.

Дії:

- Звернутися до служби підтримки банку та повідомити про підозрілу активність, заблокувати банківський рахунок та платіжні картки.
- Змінити паролі до банківських рахунків, встановити 2FA.
- Перевірити систему, в тому числі і мобільний пристрій, антивірусом чи іншою програмою із виявлення ШПЗ.
- Звернутися по допомогу до спеціалістів з інформаційної безпеки (IT-департамент, приватні фірми).

3.3. Ви помітили підозрілу активність операційної системи

- Система завантажена та зависає.
- Файли стали недоступними.
- Ви помітили файли із підозрілим розширенням.
- На робочому столі та в папках з'явилися підозрілі файли і вам відобразилось повідомлення, що Ваші файли закриптовано.

За таких обставин, Ви стали жертвою ransomware.

Дії:

- Вимкнути комп'ютер та звернутися по допомогу до спеціаліста.

Якщо ж файли все ж були зашифровані, можна спробувати визначити тип ransomware та пошукати дешифратор, хоча ймовірність повернути файли за відсутності бекапів мінімальна.

Як визначити, яким типом ransomware була інфікована система:

- Визначити розширення, яке додає файлам ransomware, це може бути «.KICK», «.crash», «.harma», «.PLUT», «.wal», «.txt», «.FREDD» та сотні інших.
- Із відкритих джерел встановити, чи було випущено дешифратор для цього типу ransomware.

АБО скористатися сайтом https://id-ransomware.malwarehunterteam.com.

3.4. Ознаки того, що мій мобільний телефон було інфіковано вірусом:

- Телефон працює значно повільніше, ніж зазвичай, зависає, батарея розряджається зазначено швидше, ніж зазвичай.
- На телефоні з'явилися іконки програм, яких ви точно не встановлювали, замість звичайного веббраузеру, запускається інший.
- Невідомі програми просять надати їм root-права (root-права – це права суперкористувача на пристроях під управлінням операційної системи "Android". Основними цілями root-прав є зняття обмежень виробника чи оператора зв'язку, маніпулювання системними програмами і можливість запуску застосунків, що вимагають прав адміністратора).
- Програми просять надати їм права чи доступ до ресурсів, які не властиві їх функціональному призначенню (наприклад, ви встановили програму «Ліхтарик» і помітили, що вона просить доступ до функції відправки або зчитування СМС, Ваших фотографій тощо. Цілком очевидно, що програмі «Ліхтарик» не потрібен доступ до текстових повідомлень та фотографій, щоб коректно працювати і, швидше за все, це вірус, який маскується під видом легальної програми).
- Ви помітили списання коштів із мобільного рахунку або/також підписки на платні сервіси.

4. ЯК МІНІМІЗУВАТИ РИЗИКИ ТА ЩО РОБИТИ, ЯКЩО Я СТАВ(ЛА) ЖЕРТВОЮ ШПЗ.

1. Використання лише ліцензійного програмного забезпечення та користування програмним забезпеченням останніх версій. Увімкніть автоматичні оновлення для операційних систем, програм. Встановлюйте та використовуйте лише те програмне забезпечення, якому довіряє Ваша організація (як приклад, використання "AppLocker").

Перелік програмного забезпечення, дозволеного для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, наведений на веб-сайті Державної служби спеціального зв'язку та захисту інформації України. Деякі із рекомендованих продуктів наведені нижче:

- «Операційна система LinuxMint версія 18.2»;
- «Комп'ютерна програма Megapolis.Документообіг 3.0»;
- Програмна система електронного документообігу «FossDoc» версії 6.x;
- McAfee Endpoint Threat Protection;
- McAfee Complete Endpoint Protection;
- McAfee Cloud Workload Security;
- McAfee Advanced Threat Defense версії 4.x;
- McAfee Network Security Platform (IPS) версії 9.x;
- ESET Enterprise Inspector версії 7.x;
- Програмний продукт антивірусного захисту «ESET Mail Security для IBM Domino Server (EMSL)» версії 7.x;
- Засоби антивірусного захисту «FortiClient»;
- Panzor Cloud Antivirus;
- McAfee MVISION Protect Standart виробництва McAfee, Inc.;
- Cisco Email Security Appliance C170, C190, C380, C390, C680, C690, C690;
- Trend Micro Deep Security версії 10.x;
- ROMAD Endpoint Defense;
- Trend Micro Enterprise Security for Endpoints Light версії OfficeScan XG;
- Symantec Data Center Security: Server, Monitoring Edition & Server Advanced версії 6.X.

Більш детальний список можна знайти за посиланням
http://195.78.68[.]84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288071&cat_id=44795
https://zakon.rada.gov.ua/rada/show/v0755388-13#Text
https://zakon.rada.gov.ua/laws/show/2163-19#Text

У випадку відсутності можливості користуватися програмними продуктами, зазначеними вище, в мережі «Інтернет» є безліч вільного програмного забезпечення, яке за функціоналом не поступається комерційному програмному забезпеченню.

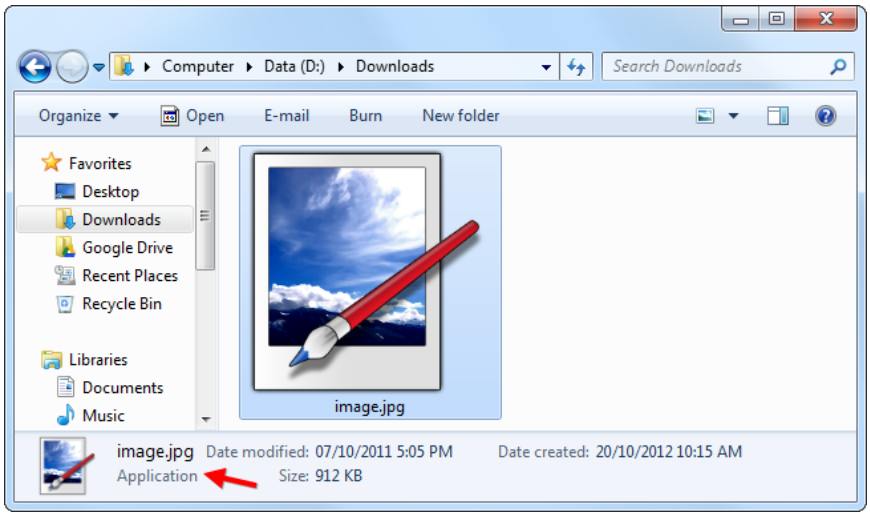
Приклади Freeware antivirus [виключити ПО РФ]:

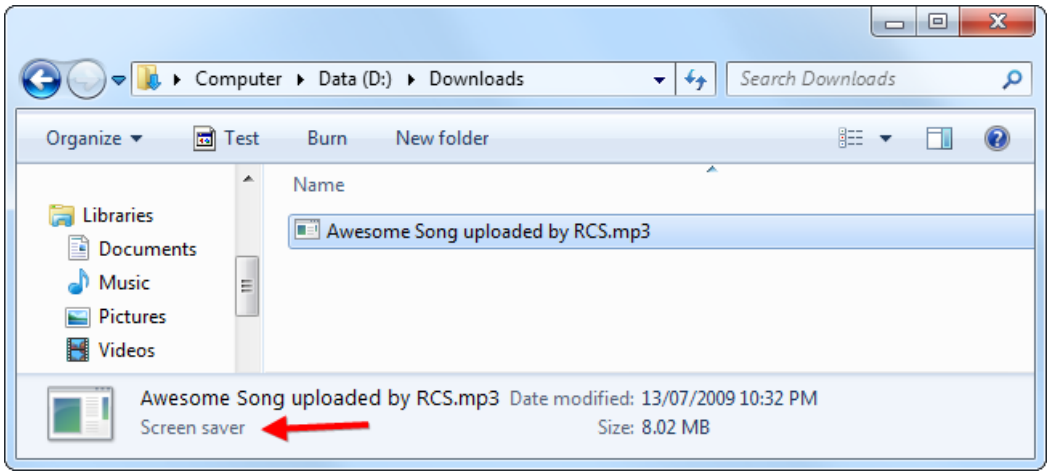
- Panda.
- Avira.
- Sophos.
- Avast.
- Bitdefender.

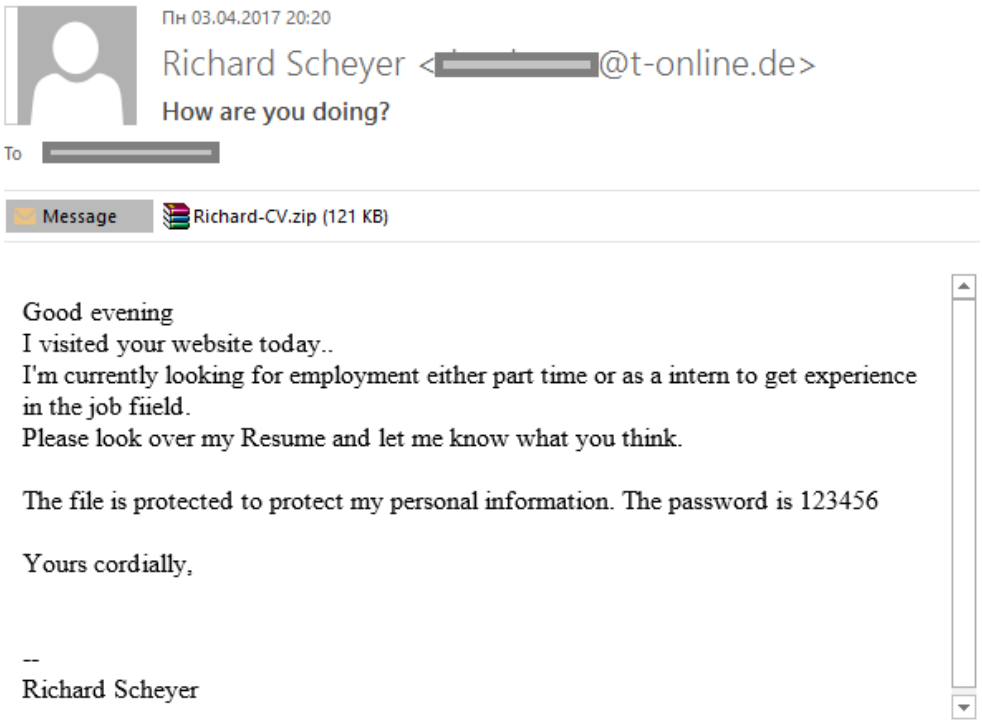
Приклади офісного програмного забезпечення:

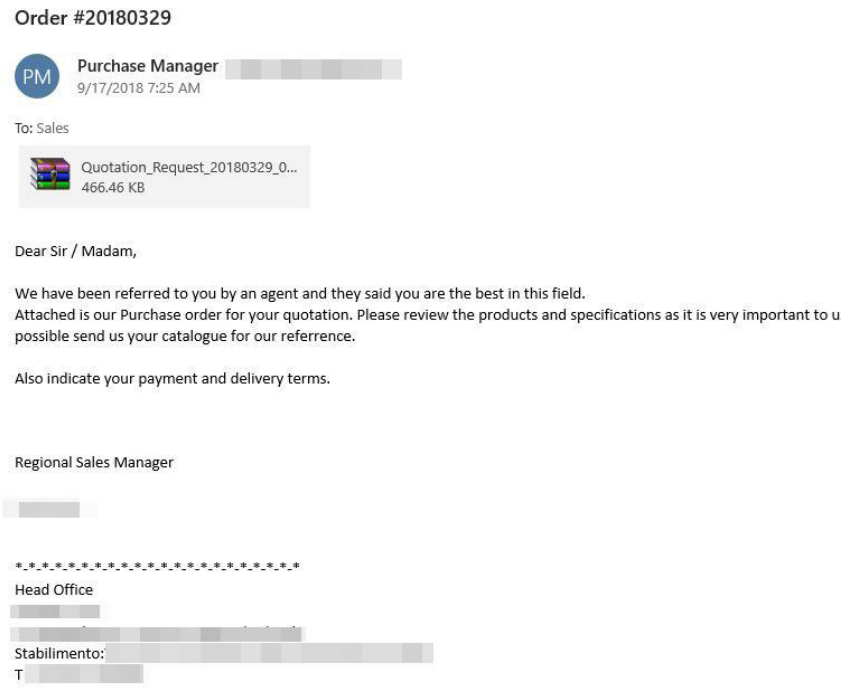
- LibreOffice.
- Foxit Reader.
- Polaris Office.
- Google Docs.

2. Не відкривайте підозрілі додатки до емейлів; не встановлюйте підозрілі розширення для інтернет-браузерів чи інші програми із сумнівною репутацією. Вимкніть використання макросів (використовуються в багатьох офісних продуктах, наприклад Microsoft Office, CorelDRAW, Notepad++); якщо Ви завантажили документ з невідомого джерела або він прийшов від невідомого чи підозрілого адресата та просить активувати макрос – **не робіть цього.** Якщо це можливо, під час використання віддаленого доступу дозволити підключення лише визначеним користувачам за допомогою «білого списку» IP-адрес (IP-whitelisting). Не користуйтеся чужими чи знайденими зовнішніми носіями інформації (флешками, дисками, тощо).




Computer ▸ Data (D:) ▸ Downloads
Search Downloads
Organize
Test
Burn
New folder
Libraries
Documents
Music
Pictures
Videos
Name
Awesome Song uploaded by RCS.mp3
Awesome Song uploaded by RCS.mp3 Date modified: 13/07/2009 10:32 PM
Screen saver
Size: 8.02 MB


Пн 03.04.2017 20:20
Richard Scheyer <[redacted]@t-online.de>
How are you doing?
To [redacted]
Message
Richard-CV.zip (121 KB)
Good evening
I visited your website today..
I'm currently looking for employment either part time or as a intern to get experience in the job fiield.
Please look over my Resume and let me know what you think.
The file is protected to protect my personal information. The password is 123456
Yours cordially,
--
Richard Scheyer



Order #20180329

PM Purchase Manager
9/17/2018 7:25 AM

To: Sales

Quotation_Request_20180329_0...
466.46 KB

Dear Sir / Madam,

We have been referred to you by an agent and they said you are the best in this field.
Attached is our Purchase order for your quotation. Please review the products and specifications as it is very important to u
possible send us your catalogue for our referrence.

Also indicate your payment and delivery terms.

Regional Sales Manager

-
Head Office
Stabilimento:
T

3. Створюйте backups де це можливо і коли це можливо [анімація як створити бекап]. Зверніться до IT-департаменту свого підрозділу, щоб довідатися про політику зберігання бекапів, та налаштувати систему збереження бекапів.

> *Backups (бекап) – процес створення копії даних з носія (жорсткого диска, дискети тощо), призначений для відновлення цих даних у разі їх пошкодження або видалення (source: https://uk.wikipedia.org/wiki/Резервне_копіювання).*

Якщо немає можливості скористатися послугами IT-департаменту, зберігайте бекапи на з'ємних носіях. В ЖОДНОМУ РАЗІ не використовуйте носій с бекапом для інших цілей. Криптуйте бекапи. Захищайте складним паролем. Зберігайте в надійному місці (сейф).

МОДУЛЬ № 5:

БЕЗПЕКА КОРИСТУВАННЯ СОЦІАЛЬНИМИ МЕРЕЖАМИ

МОДУЛЬ № 5: БЕЗПЕКА КОРИСТУВАННЯ СОЦІАЛЬНИМИ МЕРЕЖАМИ

Соціальні мережі, такі як "Facebook", "LinkedIn", "Instagram" або "Snapchat" дозволяють Вам ділитися особистою інформацією, спілкуючись з друзями, партнерами і колегами по всьому світу. Хоча мережі дозволяють Вам залишатися на зв'язку, Ви піддаєте себе ризику, що зловмисники можуть дізнатися, де Ви є, що Ви робите, чим Ви володієте та іншу інформацію.

Безпека і соціальні мережі – речі, на перший погляд, якщо не протилежні, то точно ледь сумісні. Реєструючись в соціальній мережі користувачі, за рідкісними винятками, не дотримуються анонімності. Ми ділимося фотографіями, уподобаннями в музиці, підписками на сторінки – все це елементи «профайлу», за якими нас знайдуть друзі і знайомі ... і маркетологи. А значить, всю цю інформацію можна продати.

Проблема в тому, що багато власників сервісів за гроші передадуть не лише інформацію про товари, які Ви шукали онлайн, але і більшість особистих даних. Так що інформацію, яку ви не готові афішувати на весь світ, не можна завантажувати в соціальні мережі зовсім: ні в закриті альбоми, ні в особисті повідомлення – нікуди.

У березні 2018 року стало відомо, що британська аналітична компанія "Cambridge Analytica" збирала дані користувачів через свій додаток у "Facebook" і використовувала для розміщення політичної реклами, зокрема під час президентської кампанії в США і референдуму про вихід Великобританії з Євросоюзу в 2016 році. Втручання могло торкнутися в цілому 87 млн користувачів соцмережі. "Cambridge Analytica" заперечувала свою провину, стверджуючи, що це був звичайний і законний збір даних для онлайн-реклами. Потім компанія втратила всіх клієнтів і оголосила про банкрутство. Засновник соцмережі Марк Цукерберг визнав помилку, зазначивши, що у "Facebook" зробили недостатньо для запобігання використанню її функціоналу на шкоду. "Facebook" було оштрафовано більш ніж на 5 мільярдів доларів США.

Тож в цьому модулі ми розглянемо, як варто поводитися онлайн у соціальних мережах, щоб не стати або жертвою хакерів, або «елементом статистики».

РЕЄСТРАЦІЯ

- Ви хочете використовувати своє справжнє ім'я? Деякі мережі раніше дотримувалися «політики справжніх імен», але з часом послабили вимоги.

Якщо вам не хочеться використовувати своє справжнє ім'я в соціальних мережах, можете цього не робити.

- Під час реєстрації не надавайте більше інформації, ніж потрібно. Якщо ви хочете зберегти свої контактні дані, використовуйте окрему, спеціально створену, адресу електронної пошти і не вказуйте свій номер телефону. Справжня адреса пошти і номер телефону можуть розкрити вашу особистість і зв'язати вас з іншими обліковими записами.
- Будьте обережні, вибираючи фото профілю або інших зображень, які Ви завантажуєте. Мало того, що в метаданих файлу може бути вказане місце і час зйомки, саме зображення може також розкрити будь-яку інформацію про Вас. Поставте собі питання перед завантаженням зображення: фото було знято поза межами дому або роботи? Чи видно покажчики з назвою вулиць або інші знаки і вивіски? Чи не видно робочих документів або змісту екрану комп'ютера?
- Не слід правдиво відповідати на питання для відновлення доступу до облікового запису («В якому місті ви народилися?» Або «Яке ім'я у вашого домашньої тварини?»), оскільки відповіді на такі питання можуть бути знайдені за допомогою загальнодоступних даних ваших акаунтів в соціальних мережах. Ви можете вказати довільні відповіді на ці питання. Запам'ятати ці відповіді буде важкувато, тому їх можна записати в окремому місці або зберегти за допомогою менеджера паролів.

СТІЙКИЙ ПАРОЛЬ

Захистіть Ваш обліковий запис надійним паролем. Надійні паролі довгі, складні та унікальні. Це означає, що вони повинні бути довше 10-16 символів, містити різні типи символів (літери, цифри, спеціальні символи) та бути різними для кожного облікового запису та системи. Паролі не повинні бути засновані на простих словах, які можна знайти в словниках. Паролі не повинні бути когнітивними – це означає, що вони не повинні бути засновані на даних про Вас, які можна знайти у Вашому ж обліковому записі! Дата народження, ім'я близької людини, псевдо собаки та іншу доступну інформацію не варто використовувати як складові паролю. Краще використовуйте парольні фрази, щоб уникнути проблем зі слабкими паролями.

Оберіть фразу, яку ви не зможете легко забути в наступні 2-3 дні: рядок з вірша або пісні, прислів'я, гасло тощо. Потім трансформуйте цю фразу у єдине «слово», видаливши пробіли та замінивши деякі літери схожими на них цифрами або спецсимволами: A->4, B->8, C->(, E->3, I->1, L->7, S->5, T->7 тощо. Додавання цифр та спецсимволів, а також переведення деяких букв у верхній регістр, зроблять парольну фразу ще сильнішою.

Ніхто, крім вас, не повинен знати ваші паролі та парольні фрази. Не розказуйте їх нікому, навіть дружині, батькам, дітям тощо. Ніколи не записуйте ваші паролі та парольні фрази на папері або в незашифрованому файлі. Захищений паролем файл Excel – це не шифрування. Архів, захищений паролем – не є належним шифруванням. Використовуйте надійні парольні менеджери.

Прикладами надійних парольних менеджерів є:

- 1Password https://1password.com (платний)
- Bitwarden https://bitwarden.com (безкоштовний)
- Dashlane https://www.dashlane.com/ (безкоштовний з обмеженнями)
- KeePassXC https://keepassxc.org/ (безкоштовний)

ОНОВЛЕННЯ ПАРОЛІВ ТА ПАРОЛЬНИХ ФРАЗ

Змінюйте паролі та парольні фрази на регулярній основі та принаймні один раз на рік. Паролі та парольні фрази, які ви використовуєте найчастіше (наприклад, кілька разів на день), повинні змінюватися принаймні щомісячно або раз на два місяці.

КОНФІДЕНЦІЙНІСТЬ ДАНИХ

Інформація, що зберігається третьою стороною, захищена її власною політикою конфіденційності і може бути використана в комерційних цілях і навіть передана іншим компаніям (наприклад, маркетинговим). Оскільки читання всієї політики конфіденційності – майже непосильне завдання для будь-якої людини, спробуйте ознайомитися лише з розділом, в якому йдеться про те, як використовуються ваші

дані, в яких випадках дані можуть бути передані кому-небудь ще і як компанія реагує на запити правоохоронних органів.

Сайти соціальних мереж – це, в основному, бізнес, зосереджений на отриманні прибутку. Вони часто збирають конфіденційну інформацію, крім наданої вами – де ви перебуваєте, які ваші інтереси і переваги, на яку рекламу ви реагуєте, які сайти ви відвідуєте (за допомогою кнопок «Like»).Ви можете використати розширення (плагін) браузера з блокуванням стеження для запобігання пасивної передачі зайвої інформації стороннім сайтам.

НАЛАШТУВАННЯ КОНФІДЕНЦІЙНОСТІ ТА ІНШИХ ПИТАНЬ БЕЗПЕКИ

Головна порада: змініть налаштування за замовчуванням. Наприклад, чи хочете ви ділитися своїми публікаціями з усіма або ж тільки з будь-якою конкретною групою людей? Чи можна дозволити людям шукати вас за номером телефону або адресою електронної пошти? Чи хочете ви публікувати своє місце розташування в автоматичному режимі?

Незважаючи на те, що на кожній платформі соціальних мереж є свої унікальні налаштування, ви можете помітити деяку схожість.

Налаштування конфіденційності схильні шукати відповідь на питання: «Хто може це бачити?» Тут ви зможете вибрати аудиторію («Всі», «Друзі друзів», «Тільки друзі» і т.д.) для своїх публікацій, розташування, фотографій, контактної інформації, міток і тих, хто може знайти ваш профіль через пошук.

Налаштування безпеки будуть пов'язані з можливістю блокування інших облікових записів і способів оповіщення про спроби неавторизованого доступу до вашого профілю. Іноді в цьому розділі будуть присутні налаштування входу в аккаунт: наприклад, включення двофакторної аутентифікації і резервна адреса електронної пошти/номер телефону.

Скористайтеся «перевірками» налаштувань безпеки і конфіденційності. "Facebook", "Twitter" і багато інших вебсайтів пропонують провести «перевірку налаштувань безпеки» облікового запису. Ці перевірки є чудовими покроковими настановами, описаними простою мовою. Вони дуже добре допомагають Вам відповідним чином налаштувати безпеку і конфіденційність свого облікового запису.

Пам'ятайте, що налаштування конфіденційності можуть змінитися. Іноді вони можуть ставати більш надійними і детальними, а іноді – навпаки. Звертайте пильну увагу на ці зміни: раптом інформація, раніше конфіденційна, раптово стала відкритою для всіх, або нові додаткові налаштування дозволять краще контролювати рівень вашої конфіденційності?

Ось посилання на налаштування безпеки для найпопулярніших соціальних мереж:

- Facebook https://www.facebook.com/settings?tab=security&section=approvals
- Twitter https://twitter.com/settings/security

Пам'ятайте, що більшість сучасних онлайн-сервісів підтримують двофакторну аутентифікацію. Увімкніть її за допомогою програмного коду (доступний у "Facebook", "Twitter" тощо) або за допомогою одноразового паролю з SMS. Надавайте перевагу використанню Google Authenticator, фізичного токена, або перевірці за допомогою мобільного додатку. Використання одноразових кодів через SMS менш безпечне.

Перелік сервісів, які використовують двофакторну автентифікацію доступний тут: https://twofactorauth.org/.

НЕ ДІЛІТЬСЯ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

Не використовуйте сторінку в соціальній мережі для реєстрації на сайтах, які запитують доступ до вашої особистої інформації та інформації про ваших друзів. Багато сайтів зараз пропонують авторизуватися через соцмережі, щоб проголосувати в опитуванні, залишити коментар або дізнатися результати якого-небудь тесту. Побережіть дані, обійдіться без інформації про те, яким є ваш психологічний вік або хто ви з героїв «Гаррі Поттерра».

Крім того, не анонсуйте на сторінці свої плани. Інформацією про те, що ви в найближчі вихідні збираєтеся в іншу країну, можуть скористатися квартирні грабіжники.

Пам'ятайте: все, що ви публікуєте, може бути використано проти вас!

Чим більше інформації ви публікуєте про своє особисте життя, тим легше зловмиснику налаштувати атаку проти вас. Наприклад, якщо ви публікуєте велику інформацію про свою родину, захоплення, які Вам подобаються, або про майбутню

відпустку або робочу поїздку, зловмисник може зібрати всі ці конкретні дані і створити фішингового електронного листа або телефонний дзвінок, спеціально призначений для Вас.

Якщо Ви напишете про своє улюблене проведення часу, таке як випічка, зловмисник може створити фішингових лист зі спеціальним рекламою для нового набору мисок. До цього електронного листа зловмисник може додати вкладення з купоном на 50% Вашого улюбленого бренду для випічки. **Добра порада така: якщо пропозиція здається занадто гарною, щоб бути правдою, це, ймовірно, шахрайство.**

Крім того, щоб забезпечити безпеку Вашого роботодавця, тобто держави або місцевого самоврядування, ніколи, з жодної причини не розміщуйте конфіденційну інформацію про Вашу роботу в інтернеті. Завжди звертайте увагу на те, що ви публікуєте і чим ділитеся на своїй сторінці. Слідкуйте за коментарями. Мова не тільки про коментарі, які ви залишаєте на інших ресурсах, а й про коментарі, які інші залишають на вашій сторінці. Іноді найгірший удар по онлайн-репутації посадової особи завдають не злами і «зливи» даних, а необдумані жарти, в яких хтось може побачити грубість або необережні висловлювання ваших же друзів.

БУДЬТЕ ПІДОЗРІЛИМ

Як і фішингові атаки по електронній пошті, кібер-зловмисники можуть спробувати обдурити вас в соціальних мережах. Поширений метод атаки – злочинець отримує доступ до облікового запису в соціальній мережі, наприклад, Вашого колеги. Потім Він може відправити Вам терміновий запит, наприклад, що його пограбували або Він застряг під час відпустки, і потрібні гроші, які просить відправити йому прямо зараз.

Якщо Ви отримуєте будь-які дивні або підозрілі повідомлення в інтернеті від колеги, друга або знайомого, дійте обережно і будьте обережні з відповіддю. Не відповідайте безпосередньо через обліковий запис в соціальних мережах. Замість цього зателефонуйте своєму другові по телефону, щоб підтвердити, чи дійсно він опублікував повідомлення і потребує вашої допомоги.

ЗАКІНЧЕННЯ КОРИСТУВАННЯ

Чи зможете згадати, скільки і в яких соціальних мережах ви створювали облікові записи? А яка частина з них залишаються покинутими через забутий пароль? З ростом популярності соцмереж кожен такий аккаунт може представляти інтерес для хакерів.

Отримавши доступ до закинутого аккаунту, можна використовувати його для дискредитації Вас, опублікувати рекламну і не тільки рекламну інформацію. І довіра до Вашої публікації, як посадової особи, буде набагато більшою!

Щоб уникнути цього, не забувайте про свої старі облікові записи – видаляйте за можливості або хоча б блокуйте їх. А якщо не маєте доступу, спробуйте звернутись до служб технічної підтримки по допомогу. Іноді це може спрацювати!

ВИ – ОФІЦІЙНА ОСОБА

І на останок, пам'ятайте, що Ви – офіційна особа, і навіть якщо обліковий запис Ваш особистий, все одно у користувачів буде до нього інше ставлення.

МОДУЛЬ № 6:

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ

ВСТУП

Сучасний комунікатор – це не тільки телефон!

Демонструється історичний розвиток телефонів від перших до сучасних.

У ньому органічно поєднуються функції:

- комп'ютера;
- кредитної картки;
- пристрою управління;
- мультимедіа;
- засобу зв'язку.

Така універсальність з одного боку робить виконання повсякденних завдань зручнішим, а з іншого – створює загрозу одномоментної втрати великої кількості персональних даних. В окремих випадках така втрата може стати критичною.

- *У 2019 році бізнесмен ледь не втратив мережний бізнес, який розбудовував декілька років. Спочатку зловмисники захопили управління його мобільним номером. У подальшому з використанням номера телефону бізнесмена було одержано доступ до його електронної поштової скриньки, через яку було захоплено адміністративну панель домену, який було перереєстровано на інший обліковий запис. Для зміни пароля для доступу в цьому випадку було встановлено двофакторну автентифікацію. А оскільки зловмисники захопили номер телефону бізнесмена, то, відповідно, стало можливим управління доменом. У цьому випадку бізнесмен вчасно звернувся до поліції, відповідних провайдерів та реєстраторів, завдяки чому згодом йому повернули облікові записи. Але такий результат буває далеко не завжди.*

Під час користування смартфоном Ви повинні постійно враховувати загрози, які особливо часто реалізуються в разі безтурботного ставлення до вимог безпеки. Наслідки реалізації таких загроз можуть вплинути не тільки на Вашу персональну безпеку, але й скомпрометувати підрозділ, у якому Ви працюєте, а інколи й державу загалом.

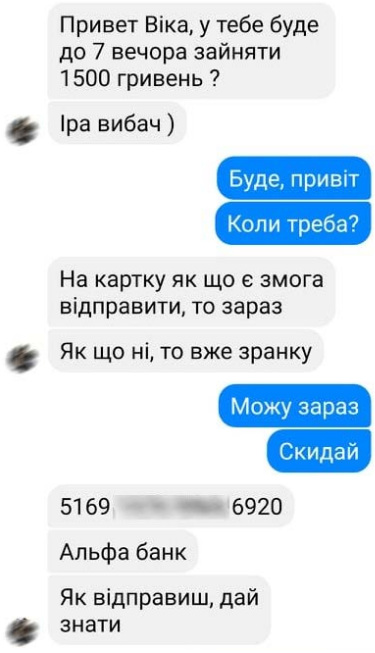
Розгляньмо декілька типових ситуацій, які можуть призвести до небажаних наслідків.

БЛОКУВАННЯ ДОСТУПУ ДО ПРИСТРОЮ

Якщо Ви залишаєте телефон без особистого нагляду, не забудьте його заблокувати надійним паролем або біометричним замком. В останньому випадку йдеться про використання як засобу автентифікації відбитку пальця або скану обличчя. У разі недотримання цих простих вимог, зловмисники можуть захопити управління не тільки Вашим телефоном, але й швидко авторизуватися в месенджерах із Вашими обліковими даними, поштових сервісах, системі онлайн-банкінгу тощо. В останньому випадку Ви можете втратити не тільки персональні дані, але й постраждати фінансово.

- *У жовтні поточного року в одній з областей України зловмисник заволодів телефоном працівниці державної установи. У подальшому за допомогою системи онлайн-банкінгу він привласнив з її банківського рахунку 40 тис. грн. Поліція встановила особу зловмисника, яким виявився неодноразово засуджений за майнові злочини молодик. Його повідомили про підозру одразу за двома статтями Кримінального кодексу України: ч. 1 ст. 187 (Розбій) та ч. 2 ст. 185 (Крадіжка).*

Може трапитися, що Ви навіть не помітите, як стали жертвою зловмисника. А в цей час Ваші облікові записи будуть успішно використовувати з протиправною метою (зобр. 1).



Зобр. 1. Використання шахраями захоплених облікових записів

Для того, щоб частково зменшити ризики потрапляння в подібні ситуації, намагайтеся використовувати там, де можливо, двофакторну автентифікацію, тобто, коли для входу до якогось мережного ресурсу потрібно ввести декілька паролів. Це може бути, наприклад, особистий пароль і додаткове підтвердження через СМС.

У будь-якому разі не ігноруйте повідомлення системи підтримки сервісів, у яких Ви зареєстровані, оскільки в таких повідомленнях може міститися інформація про сторонній вхід до вашого облікового запису або про спроби такого входу.

- *Вранці 17 травня минулого року на мобільний номер Сергія В., – одного з працівників обласної державної адміністрації, – почали телефонувати його колеги і друзі та цікавитися, що у нього трапилося і для чого йому потрібні кошти. Не розуміючи, що відбувається, Сергій почав розпитувати колег про причину таких дивних дзвінків. Виявилося, що з його облікових записів у Skype, Viber і Telegram уночі почали надходити повідомлення про те, що йому терміново потрібні гроші, а також вказано номер банківської платіжної картки, куди слід переказати кошти.*

Як потім виявилося, попереднього дня Сергій забув телефон на роботі і хтось, скориставшись його незапароленим пристроєм, спробував вчинити неправомірні дії.

Зловмисника встановити не вдалося.

У разі потрапляння у згадані ситуації терміново:

- заблокуйте найбільш чутливі облікові записи (банківські, службові електронні кабінети);
- зверніться до особи, яка відповідає за безпеку у Вашій установі (підприємстві, організації) та повідомте її про компрометацію облікових записів;
- якщо дозволяють налаштування, завершіть усі активні сеанси у Ваших облікових записах та змініть паролі.

- *Для того, щоб пересвідчитись, що Ваші облікові дані не скомпрометовано, скористайтеся одним або декількома з наведених сервісів:*

  https://breachalarm.com/
  https://ghostproject.fr/
  https://haveibeenpwned.com/
  https://leakcheck.appspot.com/
  https://monitor.firefox.com/
  https://sitecheck.sucuri.net/
  https://www.dehashed.com/

Крім наведеного, зловмисники здатні, скориставшись Вашим незаблокованим пристроєм, одержати доступ до його історії, а також до історії вже наявних облікових записів. Це може дозволити порушникам встановити місця Вашого частого перебування, коло інтересів, фінансовий стан тощо.

- *Спробуйте скористатися ресурсом takeout.google.com, який призначений для завантаження історії облікового запису Google. Як запитуваний обліковий запис використайте активний запис для телефона під управлінням операційної системи Android.*

БЕЗПЕЧНА РОБОТА В МУЛЬТИМЕДІЙНИХ ЗАСОБАХ СПІЛКУВАННЯ

Залишення телефонного пристрою незаблокованим є не єдиною загрозою. Сьогодні телефони часто використовують не тільки для класичного мобільного зв'язку, але і як комп'ютер, на якому встановлено різні мультимедійні засоби спілкування. Найпоширенішими месенджерами переважно є "Telegram", "Viber", "WhatsApp".

Деякі з наведених засобів дозволяють паралельне підключення з декількох пристроїв, як-от: комп'ютера, телефона, планшета. З одного боку, це досить зручно для користувача, а з іншого – створює додаткові ризики з погляду безпеки. Якщо, наприклад, Ви авторизуєтесь зі стороннього пристрою у своєму обліковому записі та випадково забудете вийти з нього після завершення роботи, то існує ризик подальшого використання зловмисниками облікового запису з неправомірною метою.

Найчастіше не виходять зі своїх облікових записів удома, на робочому місці, у місцях проведення інструктивних занять, у комп'ютерних класах навчальних закладів, у комп'ютерах колег або знайомих, які використовували з метою вирішення якихось короткострокових завдань.

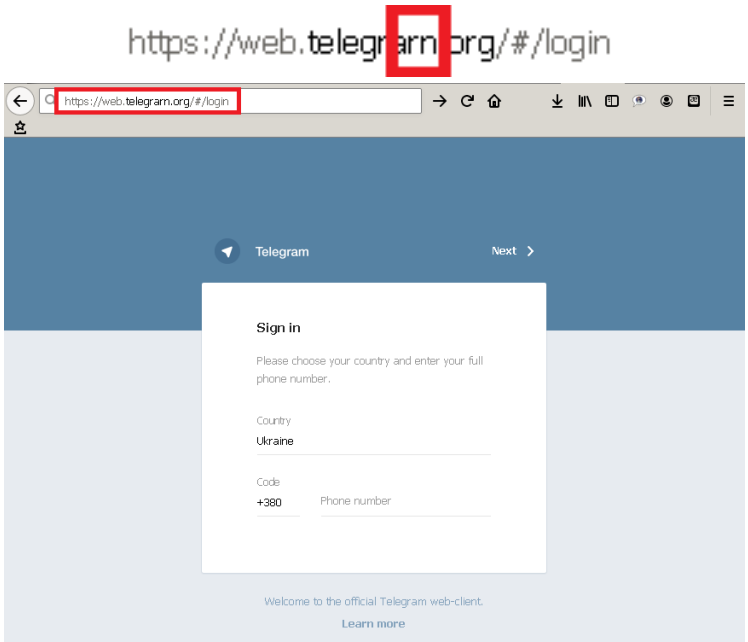
Ще однією вельми поширеною помилкою є перехід за неперевіреними посиланнями, які Вам надсилають у засобах спілкування. Окрім вірусів, такі посилання можуть містити перехід на фішінгові сервіси, призначені для введення в оману користувачів. Сьогодні існує дуже велика кількість подібних рішень не тільки для вебсайтів, але й для заволодіння управлінням месенджерами, що є вкрай небезпечно.

Наприклад, якщо у месенджері "Telegram" Вам надійде повідомлення такого вигляду:

https://t.me/@fdsgdxsfdfdgvcg.tw,

то з першого погляду воно може здатися безпечним, адже є посилання на захищене з'єднання https зі справжнім сайтом Telegram t.me. Однак насправді після натискання на таке посилання у браузері відбудеться переадресація на сайт зловмисника fdsgdxsfdfdgvcg.tw.

Фішінгове посилання може мати й не такий незрозумілий вигляд, як уже наведене (зобр. 2).



Зобр. 2. Приклад фішінгового сервісу Telegram

Враховуючи викладене, коли переходите за посиланнями, де Вас просять ввести якісь дані, уважно передивіться текст посилання на предмет його справжньості.

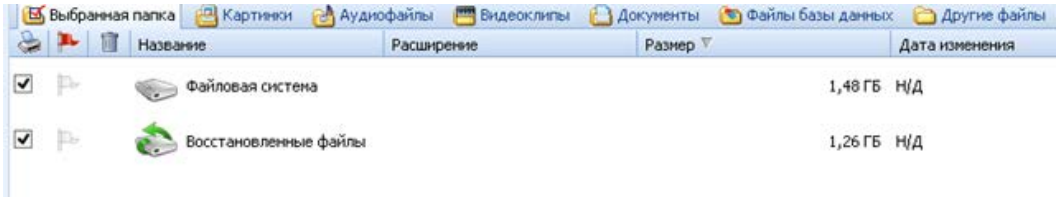
ПЕРЕДАВАННЯ ВЖИВАНИХ МОБІЛЬНИХ ПРИСТРОЇВ ІНШИМ ОСОБАМ

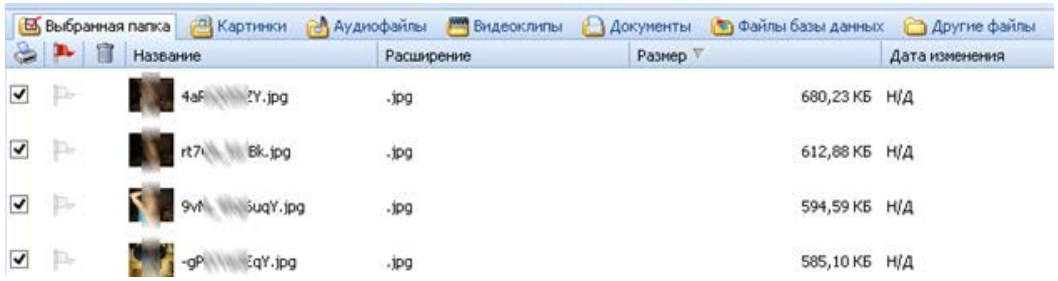
Досить необачно вважати, що описані загрози є вичерпними. Уявіть ситуацію: Ви хочете придбати новий телефон, водночас вважаєте за доцільне одержати якісь кошти від продажу старого. Тому виставляєте його на продаж через систему OLX або просто продаєте на ринку.

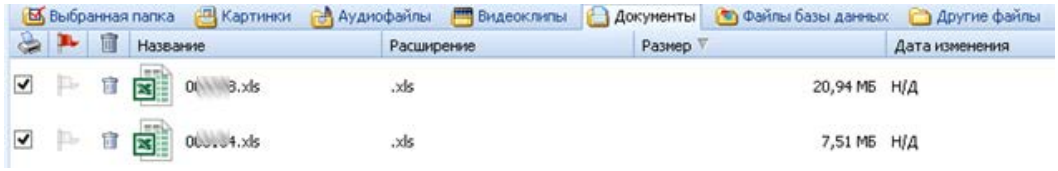
Така ситуація трапляється досить часто, однак мало хто замислюється над тим, що разом зі старим телефоном новий покупець може одержати доступ до Ваших персональних даних.

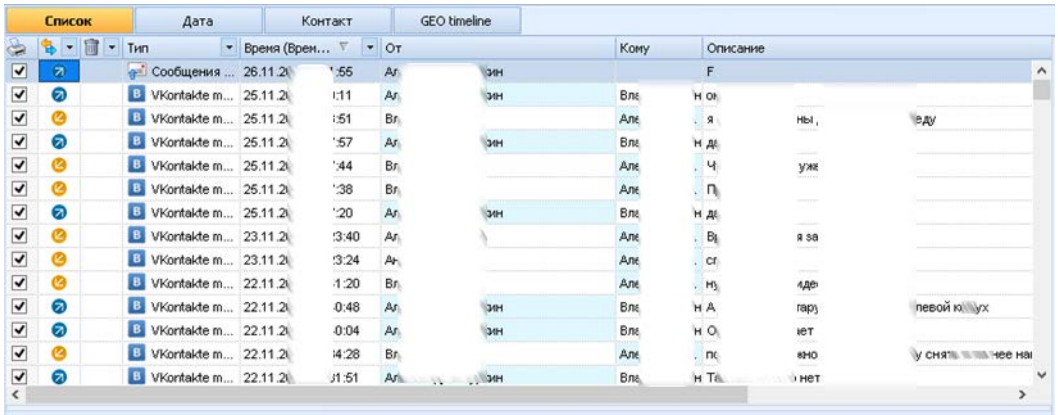
Продемонструємо це на практиці.

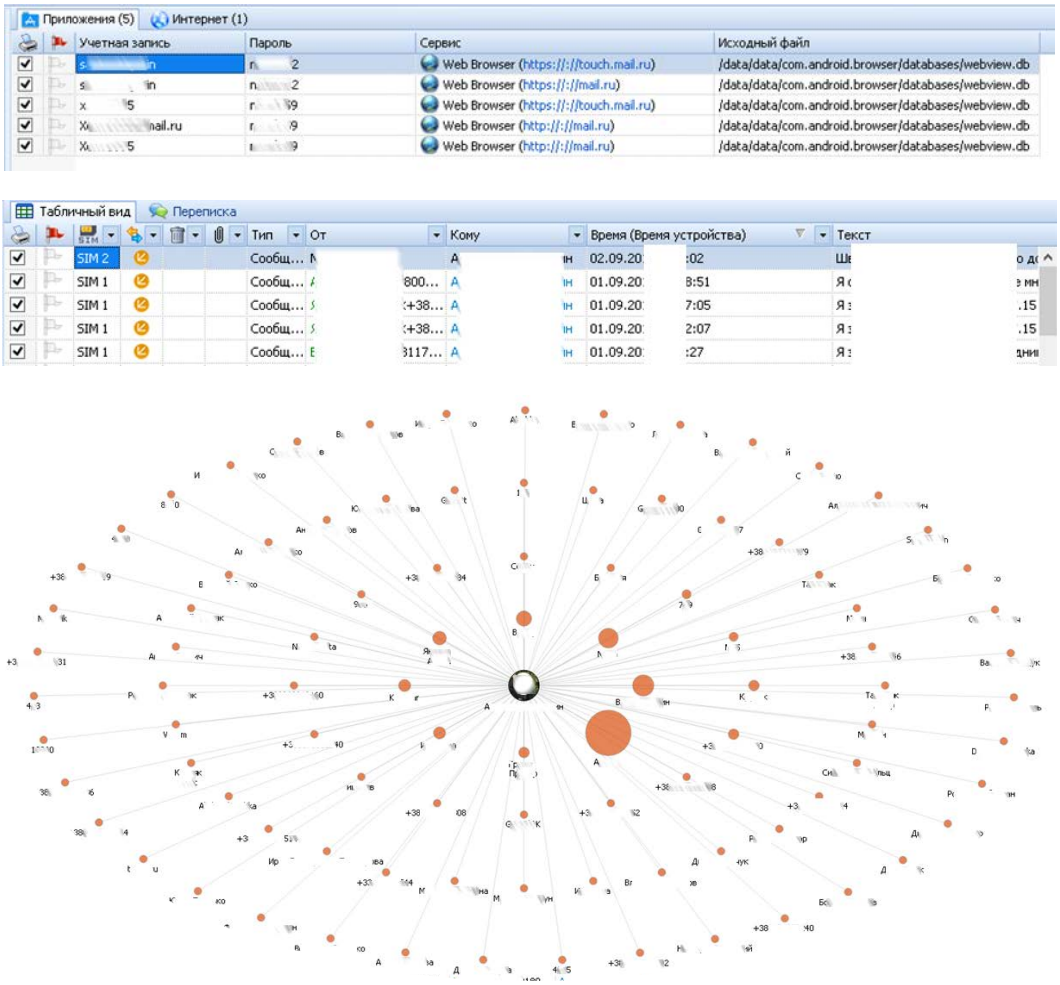
Через систему OLX придбано вживаний смартфон марки LG, у якому попереднім власником було видалено усі персональні дані. За допомогою спеціалізованого програмного забезпечення для криміналістичного дослідження мобільних пристроїв було знято образ даних смартфона. За результатами пошуку інформації, в образі вдалося виявити паролі доступу до точки доступу Wi-Fi та електронної пошти, частину листування в соціальних мережах, окремі фотографії, які зберігалися у смартфоні, повністю відновлено телефонну книгу до її видалення тощо (зобр. 3).











Зобр. 3. Результати відновлення даних із мобільного пристрою

Для того, щоб унеможливити подібні ситуації, потрібно або взагалі не передавати іншим особам свої старі мобільні пристрої, або використовувати спеціалізоване програмне забезпечення для видалення персональних даних.

Крім наведеного, під час продажу самого мобільного пристрою Ви можете зіткнутися з іншими загрозами, які реалізуються знов-таки через мобільні пристрої.

- *У 2020 році мешканка Львова Тетяна Л. вирішила продати свій мобільний телефон Samsung S8 через систему OLX за 5000 грн. За деякий час до неї надійшла пропозиція від дівчини Аліни придбати телефон за 4800 грн.*

Телефон домовилися відправити поштою з післяплатою до м. Одеса. Наступного дня до Тетяни зателефонував чоловік, який представився працівником служби технічної підтримки поштової компанії та повідомив про помилку у введенні даних отримувача і про те, що зараз вони їх виправлять, а Тетяні потрібно продиктувати СМС із підтвердженням цієї операції.

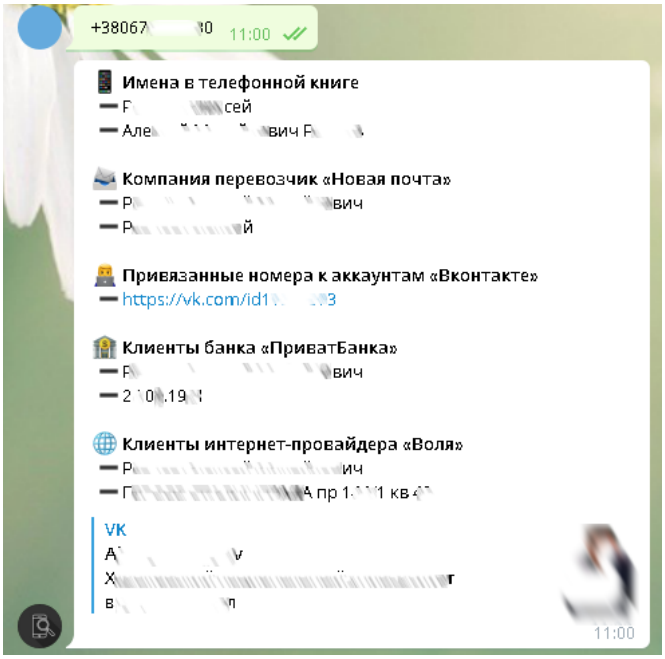
За допомогою цього коду шахраї увійшли в особистий кабінет Тетяни на сайті поштової компанії та скасували післяплату У такий спосіб вони одержали телефон без оплати, а Тетяна втратила і телефон, і гроші.

Після подання скарги до поштової компанії її представник повідомив, що така ситуація трапилася в їхній компанії вперше.

ПЕРЕДАВАННЯ КОНТАКТНОЇ ІНФОРМАЦІЇ ІНШИМ ОСОБАМ

Взагалі слід якомога менше ділитися своїми персональними даними з іншими особами. Адже це теж підвищує ризик встановлення зловмисниками Ваших повних персональних даних, які потім можуть бути використані з неправомірною метою.

На зобр. 4 наведено приклад (особисті дані приховано), як, маючи просто телефонний номер особи, за допомогою спеціалізованих сервісів можна зібрати на неї повне досьє.



Report for phone: +38067******0

Facebook checker

email_part:
- r******v@m***.ru
- r******v@u**.net

phone_part:
- +3806*******0

exists: true

Instagram exists: true

Skype possible accounts

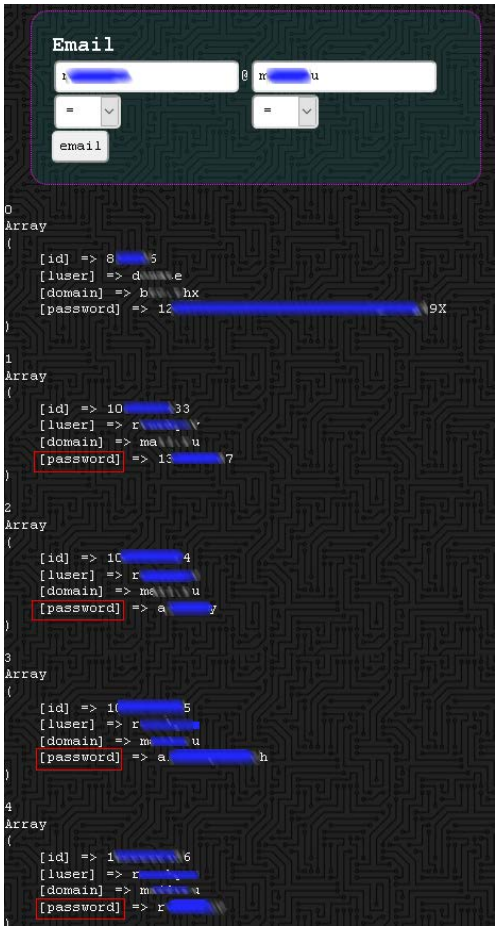
skype_profile_uid: r**********
skype_profile_deep_link: skype://r********?chat
skype_contact_type: Skype4Consumer

Telegram

firstname: O****i
lastname: R*****
telegram_profile_uid: 9*******8
lastseen: 202*-1*-1*T14:05:45

Caller ID

fullname: **
carrier: **********
country_code: **



Зобр. 4. Результати збирання даних про особу за номером телефону з використанням загальнодоступних мережних сервісів

Одержана інформація може бути використана з різними цілями. Це і шахрайство, і дискредитація, і шантаж, і створення умов для масштабної атаки на об'єкти, пов'язані з жертвою, тощо.

Зібравши інформацію про ваше коло спілкування, зловмисники можуть використати систему підміни параметра CallerID (Caller ID Spoofing). Відомими сервісами, які надають послуги із заміни CallerID, є spoofcard.com, spooftel.com. Далі порушники можуть зателефонувати Вам із будь-якого знайомого номера, наприклад, близької особи (зобр. 5) або керівника. У разі, якщо Ви не виявите підміну номера, це може призвести до незворотних наслідків.

Зобр. 4. Підміна CallerID

ЗАХОПЛЕННЯ НОМЕРА ТЕЛЕФОНУ

Під час роботи з мобільними пристроями слід пам'ятати і про іншу небезпеку, яка виходить із недосконалості системи ідентифікації власника мобільного номера. Йдеться про перереєстрацію зловмисником Вашого номера на своє ім'я через перевипуск SIM-картки шляхом повідомлення операторові даних стосовно активності номеру за певний період часу. Очевидно, що заволодівши Вашим мобільним номером, зловмисник здатен реалізувати наведені вище загрози, а також використовувати цей номер із неправомірною метою для вирішення поточних завдань.

- *О 21:00 у червні поточного року працівниця Державної фіскальної служби Галина П. одержала SMS від свого оператора про те, що відбувається заміна її SIM-картки. Вранці зв'язок припинився. Галина звернулася до сервісного центру мобільного оператора, де їй відновили телефонний номер протягом двох годин. Проте за цей час відбулося списання грошей з її банківського рахунку через систему онлайн-банкінгу.*

У цьому прикладі зловмисник скористався системою відновлення мобільного номера, алгоритм роботи якої базується на тому, що оператору потрібно вказати:

- номери, з яких найчастіше телефонували на відновлюваний номер;
- коли було здійснено останнє поповнення балансу;
- з якими номерами відбувалися останні з'єднання.

Якщо Вам часто телефонують із невідомих номерів, раптово поповнюють баланс, то це може свідчити про підготовку до зміни номера.

Для того, щоб убезпечитись від вказаної ситуації, потрібно прив'язати свій телефонний номер до паспортних даних. Крім того, бажано для чутливих операцій використовувати телефонний номер, який нікому не відомий, крім його власника та оператора зв'язку або про який обізнані тільки близькі особи.

Якщо все ж таки Ваш телефонний номер захопили, то Вам слід терміново спробувати заблокувати активні банківські платіжні картки, а якщо це не виходить, спробувати зняти з них кошти у найближчому відділенні банку чи банкоматі.

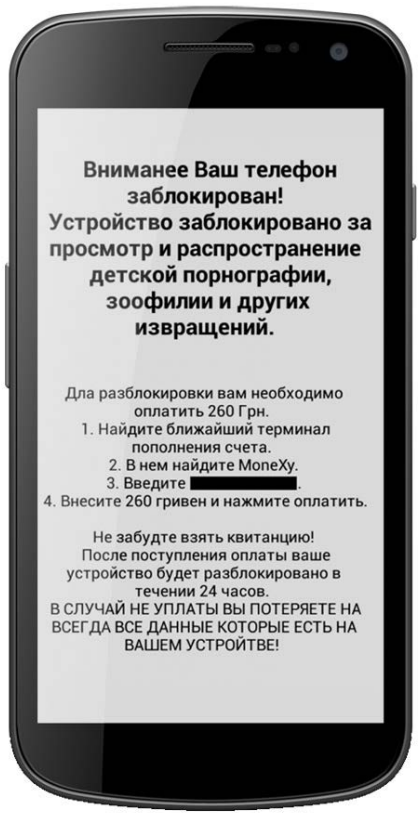
Інколи користувачі мають упевненість, що вжили усіх заходів реагування. Проте, як показує практика, жодні додаткові заходи безпеки не будуть зайвими.

- *У червні поточного року зловмисники реалізували схему заволодіння коштами особи, які зберігалися в банку, який здійснює обслуговування без відділень. У власниці мобільного пристрою iPhone спочатку було вкрадено телефон, власниця оперативно заблокувала його через інтернет на сайті Apple та вирішила, що блокувати банківську платіжну картку немає сенсу, оскільки доступ до рахунку в банку можливий тільки зі знанням PIN-коду. Проте зловмисники перевели вкрадений пристрій в режим польоту, а згодом підключили його до мережі «Інтернет» через свій маршрутизатор, на якому було обмежено доступ до сервісів Apple. Водночас банківські застосунки продовжували працювати. У такий спосіб викрадачам вдалося вивести понад 70 тис. грн. із рахунків жертви.*

ВІРУСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Вкрай небезпечним, з погляду безпеки, є потрапляння на мобільний комунікатор вірусного програмного забезпечення. Такі програми можуть виконувати різні функції. У будь-якому разі вони здатні скомпрометувати не тільки саму систему, у якій запущені, але і її власника.

Нерідко вірусне програмне забезпечення здатне спричинити неприємні наслідки у вигляді зашифровки даних телефона, перехоплення автентифікаційних даних, надсилання повідомлень на платні номери, оформлення платних підписок на різні сумнівні сервіси, використання пристрою для скоординованої атаки на різні об'єкти тощо (зобр. 6).



Зобр. 6. Приклад роботи вірусу

- *У травні 2018 року було зламано телефон одного з найбагатших людей світу за допомогою спеціального відеофайлу в месенджері WhatsApp. За декілька годин після злому зі скомпрометованого телефону було викрадено декілька особистих файлів, а фотографії бізнесмена було передано одному з таблоїдів.*

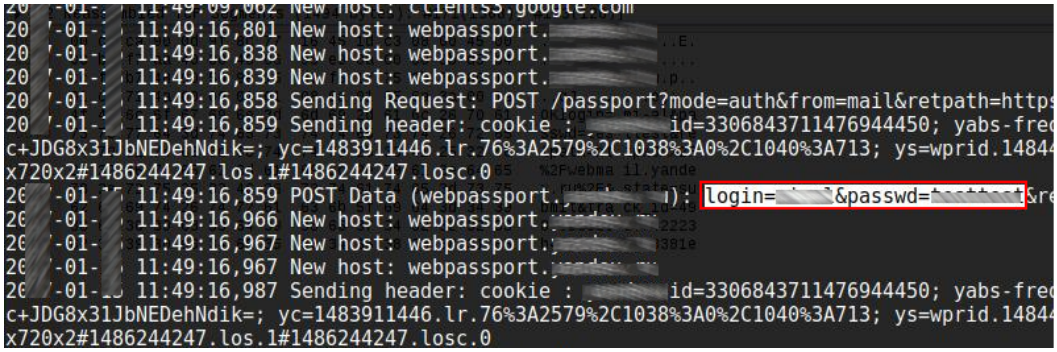
Враховуючи викладене, намагайтеся ніколи не встановлювати програмні рішення з неперевірених джерел. Інсталюйте антивірусне програмне забезпечення на свій

пристрій. Не намагайтеся без крайньої потреби отримати права суперкористувача root на своїх мобільних пристроях з використанням спеціальних програм зломщиків обмежень, встановлених виробником мобільного пристрою. З одного боку, рутинг дає змогу користувачеві зняти обмеження виробника чи оператора комунікацій, а з іншого – полегшує зловмисникам доступ до Вашого пристрою.

ДОДАТКОВІ ФУНКЦІЇ МОБІЛЬНОГО ПРИСТРОЮ

Крім наведеного, візьміть за звичку вимикати в телефоні функції, які не використовуєте.

Так, якщо у Вас налаштовано автопідключення до відомих точок доступу WiFi, то Ви так само автоматично можете бути під'єднаним до підробленої точки доступу. У подальшому весь трафік інтернету може бути пропущений через обладнання зловмисника. Це дає змогу порушнику примусово переадресовувати запити з Вашого пристрою на свої ресурси (зобр. 7). Водночас Ви можете навіть нічого не помітити.



Зобр. 7. Результат роботи програми mitmAP, призначеної для автоматизації створення бездротової точки доступу та перехоплення трафіку

Потреба вимикати невикористовувані функції стосується не тільки Wi-Fi, але й інших технологічних рішень. У даному випадку можна згадати про NFC-модуль, який дає змогу прикріпити до мобільного пристрою банківську платіжну карту та через спеціальну банківську програму здійснювати безконтактні платежі. Увімкнений NFC-модуль, наприклад, може спричинити втрату грошових коштів або зараження вірусом.

- *У 2018 році працівники компанії "Checkmarx" продемонстрували, як зламати мобільний пристрій одним дотиком. Цей спосіб зламу одержав назву NFCdrip і полягає в передаванні зі спеціального пристрою або іншого смартфона через модуль NFC вірусного програмного забезпечення на пристрій жертви.*

Варто зазначити, що від цілеспрямованих атак на мобільні пристрої не можуть бути застраховані навіть особи, обізнані з правилами інформаційної безпеки. Тому слід дуже прискіпливо ставитися до усіх незрозумілих подій з Вашим пристроєм і ретельно обмірковувати свої дії в таких випадках.

- *У 2020 році близько двадцяти керівників криптовалютних бірж Ізраїлю стали жертвами кіберзлочинців, які зламали їхні облікові записи в "Telegram". Попередньо зловмисники одержали доступ до стільникової мережі за кордоном та надіслали звідти оператору в Ізраїлі службове повідомлення про зміну місцезнаходження абонента-жертви. Після цього вони фактично змогли контролювати вхідні повідомлення жертви і в такий спосіб зламати її облікові записи.*

  У цьому випадку, очевидно, у жертв злочину не було встановлено двофакторної автентифікації, що дало нагоду зловмисникам захопити їхні облікові записи.

ГОЛОВНІ ПРАВИЛА РОБОТИ З МОБІЛЬНИМИ ПРИСТРОЯМИ

Усі наведені загрози не є вичерпними. Слід враховувати, що вони відображають тільки декілька ризиків. Але водночас постійно з'являються нові вразливості й атаки, які можна відстежити тільки в процесі самоосвіти.

Тим не менш, для забезпечення прийнятного рівня безпеки слід дотримуватися базових правил:

1. Встановити PIN-код на SIM-картку для того, щоб, у разі її втрати, зловмисники не змогли її використати з неправомірною метою.

2. Де можливо, використовуйте двофакторну автентифікацію.

3. Активуйте у смартфоні функції «Знайти телефон». Якщо Ви втратите телефон, то в подальшому це може допомогти оперативно встановити місцезнаходження втраченого пристрою.

4. Не прикріплюйте всі банківські платіжні картки до єдиного телефонного пристрою. У разі втрати пристрою Вам не доведеться блокувати всі платіжні картки.

5. Встановіть складний пароль на доступ до пристрою та увімкніть біометричну автентифікацію.

6. За можливості, не вмикайте в телефоні функцію Smart Lock (розблокування за допомогою сторонніх пристроїв, як от наприклад, смарт-годинник). Зловмисники можуть скористатися цією функцією для зламу Вашого пристрою.

7. Слід вимкнути функцію виведення повідомлень на заблокований екран:

iOS: «Налаштування» → «Повідомлення» → «Показ мініатюр» → «Ніколи».
Android: «Налаштування» → «Повідомлення» → «Повідомлення (Екран блокування)» → «Приховати вміст».

8. Не створюйте та не пересилайте за допомогою месенджерів і повідомлень телефону скан-копії важливих документів, інтимні фотографії.

9. Якщо Вам хтось надсилає повідомлення або телефонує з проханням термінового переказу коштів, візьміть паузу, все добре обдумайте. За можливості, передзвоніть іншим особам, пов'язаним із запитувачем, а також йому самому, та переконайтеся, що це саме та особа, про яку Ви думаєте. У подібних ситуаціях намагайтеся не пересилати кошти на карти чи електронні гаманці, краще передати їх особисто.

10. Якщо змінюється номер мобільного телефону, потрібно не забути перереєструвати всі наявні облікові записи на новий номер.

11. Якщо телефон було втрачено, потрібно терміново звернутися до оператора телекомунікацій та заблокувати SIM-картку, заблокувати банківські платіжні картки. Надішліть повідомлення на сайти мікрофінансових установ про те, що ваш телефонний номер було втрачено. У разі потреби, зверніться до поліції. Повідомте про інцидент безпосереднього керівника та особу, яка відповідає за безпеку у Вашому підрозділі. Поділіться із колегами досвідом розв'язання інциденту, пов'язаного з порушенням інформаційної безпеки.

МОДУЛЬ № 7:

ФІЗИЧНА БЕЗПЕКА

МОДУЛЬ № 7: **ФІЗИЧНА БЕЗПЕКА**

Фізична безпека є невід'ємною частиною захисту установи від втручання в роботу її комп'ютерних систем. Але чому? Справа в тому, що, маючи фізичний доступ, порушник може безпосередньо взаємодіяти із системою та обійти існуючі механізми захисту.

Тому, у цьому розділі ми поговоримо про загрози, пов'язані з недотриманням правил фізичної безпеки, та яких рекомендацій ми мусимо дотримуватись аби зберегти безпеку своєї установи.

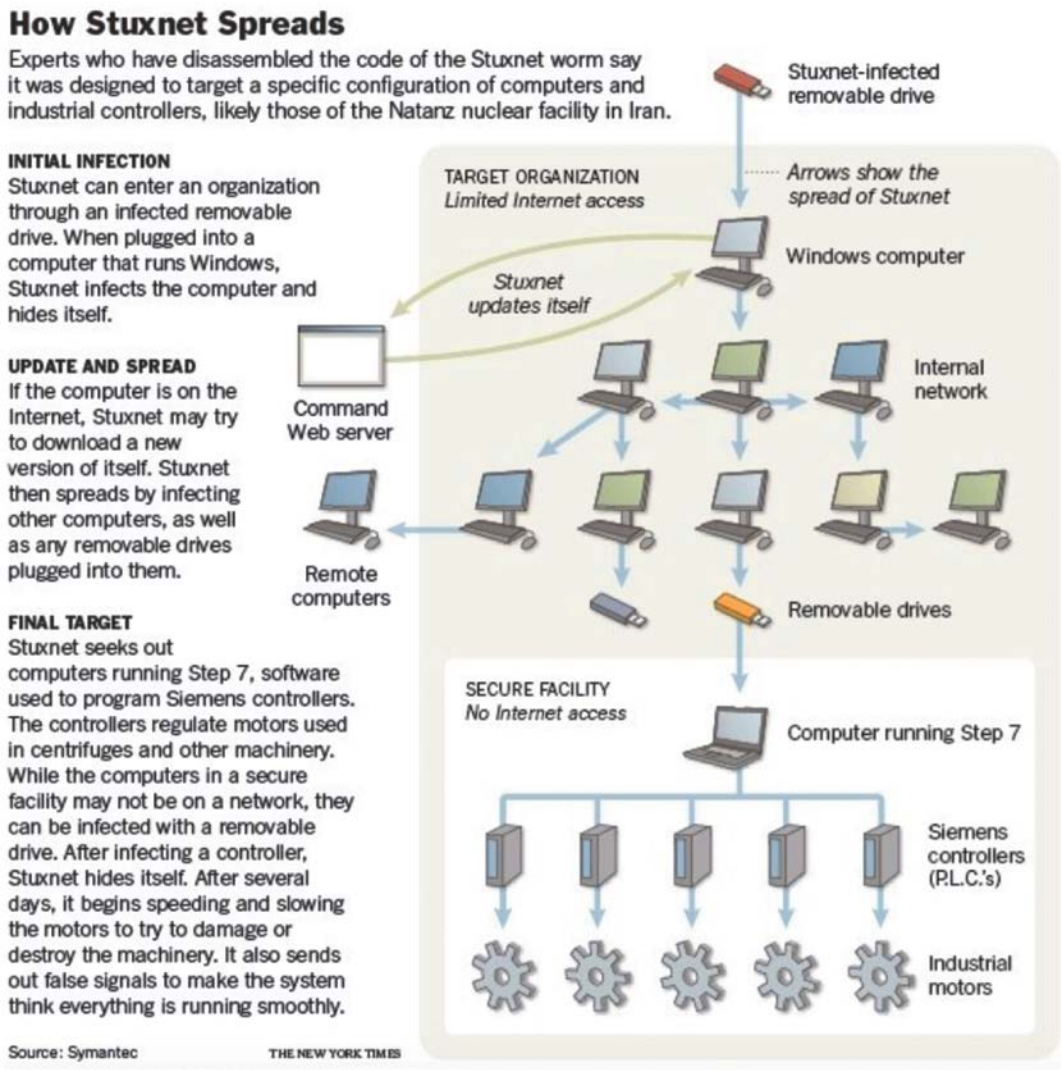
Найпопулярніша атака через фізичне втручання: Stuxnet

У 2009 році Іранські заводи у місті Натанзе, які збагачували уран в рамках ядерної програми, зазнали безпрецедентної кібератаки. Було заражено близько 200,000 комп'ютерів та 1000 одиниць спеціального обладнання було виведено з ладу.

Згідно зі звітом "Business Blackout" збитки становили близько $243 мільярди та змусили Іран припинити свою ядерну програму.

Цікавий факт: вищезгадані об'єкти не були підключені до мережі «Інтернет». Тож як злочинцям вдалось доставити шкідливий програмний код?

Відповідь: за допомогою флеш носія, який співробітник заводу вставив у свій комп'ютер. І це питання фізичної безпеки.



КОНТРОЛЮВАННЯ ЗОВНІШНЬОГО ФІЗИЧНОГО ПЕРИМЕТРУ (ЗЛОВМИСНИК ПОЗА ПЕРИМЕТРОМ)

Зловмисники можуть спробувати пробратись на територію установи, до якої доступ мають тільки авторизовані люди. У цій темі ми поговоримо, які методи використовують злочинці, аби проникнути всередину вашої організації та як запобігти цьому.

СТОРОННІМ ВХІД ЗАБОРОНЕНО

Раніше ми з Вами говорили про принципи соціальної інженерії та як хакери користуються людською психологією, аби отримати бажаний результат: змусити відкрити файл або перейти за посиланням. Втім ці самі принципи використовуються для отримання доступу в середину організації.

«ВПАСТИ НА ХВІСТ» – TAILGATING

Одним з таких прикладів є так званий «вхід на плечах» – англ. (tailgating). Зловмисник намагається приєднатись до групи авторизованих осіб, які заходять до будівлі, видаючи себе за людину, яка теж працює у цій установі.

«ЗАЙНЯТІ РУКИ»

Люди схильні допомагати один одному. Але чи завжди це потрібно?! Зловмисники розуміють/знають цю людську природу та користуються нею. Як ви бачите на малюнку, людина з кавою видає себе за авторизовану особу та ніби не має можливості відчинити двері. Вона сподівається, що авторизовані особи поведуться та пропустять, відкриваючи двері/турнікет своєю карткою.

“ДОСТАВКА”

Інший метод несанкціонованого проникнення на територію організації – видати себе за доставку/працівників інтернет-провайдера тощо.

ПІДСУМОК

- Перевіряйте особистість людини, яка намагається потрапити до будівлі.
- Пам’ятайте, що допомагати – добре. Але інколи цим можуть скористатись.
- Якщо ви не чекали доставку/працівників інтернет-провайдера, зателефонуйте їм, щоб переконатись.

ЗЛОВМИСНИК ПОРЯД З ВАМИ. РЕЧІ БЕЗ НАГЛЯДУ

Крадіжка власності для отримання інформації

Однією з перших загроз є крадіжка власності.

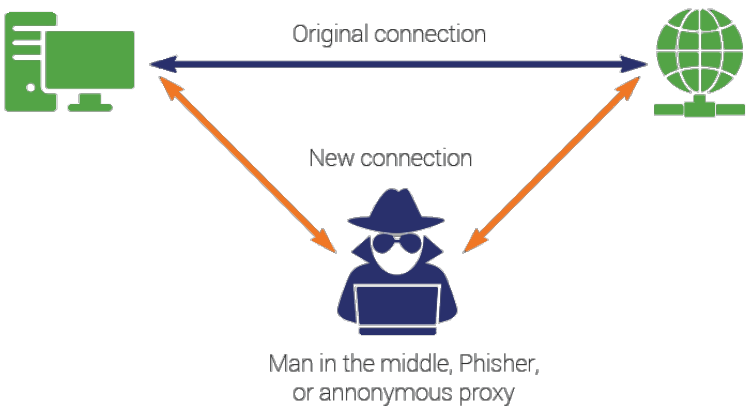
Встановлення віддаленого доступу

Чому, сидячи у кав’ярні або на робочому місці, ми не маємо залишати свої пристрої без нагляду, а тим паче не блокуючи їх? Окрім крадіжки Вашої власності або власності Вашої організації, ви даєте можливість зловмисникам отримати віддалений контроль над вашим пристроєм.

Маючи фізичний доступ до Вашого комп'ютера, порушник потребує всього декілька хвилин для того, щоб створити віддалений доступ до цього пристрою (бекдор).

Людина посередині (man-in-the-middle)

Маючи доступ до вашого комп'ютера, зловмисник також може зробити деякі налаштування, які дозволять йому/їй перехоплювати весь трафік з вашого пристрою. Таким чином, він/вона зможе бачити всю вашу службову та особисту комунікацію, паролі, відвідувані сайти, всі фотографії, банківські дані тощо.



Встановлення HTTP proxy (без тех. визначень) просто пояснити, що на це потрібно декілька хвилин, але це надасть можливість злочинцю бачити весь трафік.

Деталі про встановлення сертифікатів тощо – обговорюватись не буде.

ПІДГЛЯДАННЯ (SHOULDER SURFING)

Підглядання (англ. shoulder surfing) – техніка соціальної інженерії, яка використовується для отримання інформації від конкретного користувача.

Зазвичай ця техніка використовується для отримання конфіденційних даних жертви: дані облікових записів, пін-коди банківських карток, паролі для розблокування пристроїв, особисте листування тощо. Для виконання цієї техніки не потрібні специфічні навички, лише спритність та підготовка того, хто її виконує.

На що полюють зловмисники?

Дані банківських карток

Паролі облікових записів / для розблокування пристроїв

ФІЗИЧНИЙ ДОСТУП ДО МЕРЕЖІ

Чому надати пароль від Wi-Fi – погана ідея?

Wi-Fi мережа – ваш дім. Надаючи пароль від Wi-Fi стороннім особам, ви надаєте доступ до середини вашого дому і можливість взаємодіяти з іншими пристроями.

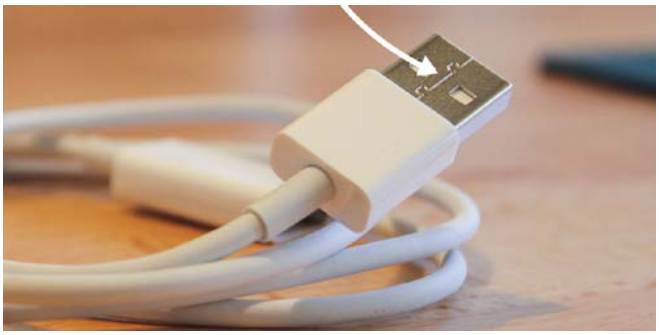
ФЛЕШ НОСІЇ ТА ВИКОРИСТАННЯ USB
ЗАРАЖЕННЯ ЧЕРЕЗ ФЛЕШ-НОСІЇ

У минулих розділах ми з вже говорили про шкідливе програмне забезпечення (ШПЗ) та його можливості/можливі наслідки. Ми згадували, що зловмисники часто використовують електронну скриньку для доставки шкідливого коду, але так є не завжди.

Флеш-носії також слугують чудовим інструментом для запуску шкідливих програм на комп'ютері, тому ми маємо до них ставитись з обережністю.

Чому флеш-носії такі небезпечні?

- відкриваючи файли з флеш носія, Ви запускаєте процес на своєму комп'ютері, який може нанести шкоду вам та вашій організації в цілому.
- деякі флеш-носії/usb кабелі можуть автоматично виконати код і не потрібно навіть нічого відкривати.



Пам'ятайте: зловмисники намагаються використовувати принципи соц. інженерії, щоб підвищити шанси запуску файлів на флеш-носіях.

Стереотипи:

- якщо просто відкрити файл, нічого ж не відбудеться;
- операційна система сама себе захистить;
- антивірус завжди покаже зараженість носія/usb кабелю.

Дослідження

2015 року дослідниками з компанії "Google", Університету Іллінойс та Університету Мічиган було проведено дослідження щодо популярного методу доставки ШПЗ – через флеш носії.

У рамках експерименту, дослідники розкидали 297 флешок (різних на вигляд – зобр. нижче) на території університетів з метою аналізу поведінки людей та визначення успішності такої атаки.

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Важливо зазначити, що цільова аудиторія була технічно обізнана.

Результат дослідження показав, що 98% людей забрали флеш носії та 48% відкрили файли.

Найкоротший проміжок часу від моменту підняття до відкриття файлу становив 6 хвилин. Середній час – 6.9 годин.

68% опитаних сказали, що хотіли повернути пристрої власникам, а 18% сказали, що їм був цікавий зміст файлів. Деякі користувачі зазначили, що флеш носії з ключами спонукали їх знайти власника.

«Хтось не зможе потрапити до квартири/дому, тому я хотів повернути його якомога швидше».

Отже, як ми бачимо з дослідження, метод доставки ШПЗ через флеш-носії дуже дієвий. Користуючись людською психологію і бажанням допомогти/цікавості, зловмисники можуть успішно отримати віддалений контроль над пристроєм та реалізувати інші атаки, які ми порушували у цьому курсі в розділі про ШПЗ.

ШИФРУВАННЯ КОМП'ЮТЕРА (ОФЛАЙН ЗУСТРІЧ?) ЯКИХ ПРАВИЛ ДОТРИМУВАТИСЬ

- Контроль фізичного периметра;
- Перевіряйте особистість людини, яка намагається потрапити до будівлі;
- Пам'ятайте, що допомагати – добре. Але інколи цим можуть скористатись;
- Якщо Ви не чекали доставку/працівників нтернет-провайдера, зателефонуйте їм, щоб переконатись;
- Не залишайте сторонніх людей без супроводу;
- Зачиняйте за собою двері;

- Речі без нагляду
- Не залишайте свої пристрої без нагляду;
- Налаштуйте автоматичне блокування ваших пристроїв та блокуйте завжди ваш комп'ютер, якщо не користуєтесь ним.

Як налаштувати?

На Windows:

- Відходиш від робочого місця? натискай – Windows+L ;
- Натисніть Ctrl-Alt-Del та виберіть «Заблокувати» ;
- Налаштуйте автоматичне блокування після 5 хвилин відсутності активності.

Mac:

- Command+Control+Q;
- Яблуко у верхньому лівому куті – «Заблокувати екран»;
- «Налаштування» -> «Безпека та приватність» -> «Вимагати пароль відразу».
- Коли вводиш секретні дані (паролі від облікових записів, банківські дані та іншу персональну інформацію), прикривай введені значення рукою.
- Політика чистого столу. Не залишай на столі важливих документів, паролів тощо.
- Не використовуйте пристрої, яким не довіряєте (чиє джерело вам не відоме).

МОДУЛЬ № 8:

УБЕЗПЕЧЕННЯ ВІД НЕПРАВДИВИХ ПОВІДОМЛЕНЬ

МОДУЛЬ № 8: УБЕЗПЕЧЕННЯ ВІД НЕПРАВДИВИХ ПОВІДОМЛЕНЬ

«Частіше мийте руки після контактів з відомою пропагандою»

В. Зеленський[6]

ВСТУП

Ви, напевно, неодноразово чули фразу про те, що той, хто володіє інформацією, володіє світом. Сьогодні ця теза, як ніколи, є актуальною. Технології неправдивих повідомлень для впливу на маси почали активно використовувати у XX ст. (зобр. 1).

Зобр. 1. Видалення з фото учасника першого загону космонавтів Григорія Нелюбова

Але якщо раніше для цього залучалися професійні команди, то сьогодні із появою різних комп'ютерних технологій та мережі «Інтернет» буквально кожен більш-менш обізнаний користувач може створювати фейкові повідомлення та поширювати їх. Згадайте, наприклад, як за допомогою фоторедакторів Ви або Ваші знайомі редагували зроблені фотознімки. Із появою штучного інтелекту проблема лише поглибилась. Сьогодні за допомогою відповідних програм[7] досить легко зробити не тільки неправдиве фото (зобр. 2), але й відео, яке буде виглядати як справжнє.

[6] Zelenskiy / Official. URL: https://t.me/V_Zelenskiy_official (дата звернення: 06.11.2020).

[7] The best Deepfake apps in 2020 which you can use for fun. Lets know more about the mind bending AI technology. URL: https://nextalerts.com/2020/08/16/the-best-deepfake-apps-in-2020-for-fun/ (дата звернення: 08.11.2020).

Зобр. 2. Зображення, створені за допомогою штучного інтелекту, зліва направо: зображення неіснуючої людини, створене за допомогою сервісу thispersondoesnotexist.com; портрет створений на основі першого фото за допомогою сервісу ai-art.tokyo; мультяшний персонаж на основі першого фото, створений за допомогою бота Telegram @picaibot.

Як не заблукати в мережі, відрізнити правду від вимислу? Саме цим питанням присвячено дану тему.

ВИДИ МАНІПУЛЯЦІЙ

Перенесення переважної кількості інформаційних потоків в мережу «Інтернет», з одного боку, значно полегшило доступ користувачам до різних відомостей і знань, а з іншого – створило велику кількість можливостей для маніпуляції з боку правопорушників. Такі маніпуляції можуть бути спрямовані на окремих осіб, групи, створювати передумови для формування «потрібної» громадської думки.

Маніпуляції можуть бути *свідомими* або *несвідомими*, проте вони все одно здатні вплинути на прийняття рішень як звичайними користувачами, так і керівним складом державних органів.

Одним із найбільш поширених прикладів подібних відомостей є інформаційні сторінки, що містять інформацію з минулого, але позиціонуються як новина дня.

- *01 листопада 2020 року в мережі «Інтернет» було розміщено новину про те, що доларові депозити завдають їхнім власникам збитки, у той час як гривневі є більш прибутковими[8]. Проте, якщо уважно проаналізувати зміст повідомлення, стає зрозуміло, що це новина 2013 року, і сьогодні вона може бути зовсім не актуальною.*

[8] Долларовые депозиты приносят их держателям одни убытки, в то время как вклады в гривне дают более значительную доходность. URL: https://web.archive.org/web/20201106213245/https://telegraf.com.ua/biznes/finansyi/amp-656615-depozityi-v-grivne-vyigodnee-chem-v-dollarah.html (дата звернення: 06.11.2020).

Неправдиві ресурси часто називають фейками. Фейк може бути візуальним, для чого використовуються графічні та відеоредактори. У межах інформаційного впливу під час доведення до відома інформації використовується певний набір характеристик: видовищність, порушення звичної моделі світу, примушуюча пропаганда, «наклеювання ярликів», «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг[9]. Типові ознаки троля: емоційні меседжі, чіткі тези із закликами, одноманітний профіль у мережі, незначна кількість віртуальних друзів, відсутність власних постів, створена нещодавно сторінка[10].

У мережі «Інтернет» найбільш частими каналами для поширення фейків є вебсайти новин, соціальні мережі, блоги, розсилки електронною поштою.

- *У жовтні 2020 року в мережі «Інтернет» низка ЗМІ поширила повідомлення про те, що президент Туреччини не визнає Крим російським, оскільки вважає, що півострів належить його країні. Ця інформація з'явилася на фоні просування Міністерством закордонних справ України ідеї створення «Кримської платформи», покликаної вирішити питання деокупації Криму.*

  У відповідних матеріалах ЗМІ посилалися на турецьке видання "Haberler", в одній з новин якого була стаття із розділом «Ердоган бажає, щоб Крим віддали Туреччині». У цьому розділі видання посилається на фрагмент статті з газети «Московський комсомолець», у якій її автор зробив припущення про позицію президента Туреччини. Таким чином, в результаті маніпуляції припущення, яке пройшло через низку «фільтрів», у підсумку було подано як факт. Згодом інформацію було спростовано[11], але не всі звернули на це увагу.

У 2018 р. О. Юркова на підставі сучасного практичного досвіду представила декілька способів створення недостовірних новин[12]. Серед них:

[9] Зеленина Е. В Королевстве кривых зеркал… *Время*. Вторник. Декабрь 17 2013. № 181 (17337). с. 2.

[10] Іванцова А. Інтернет-тролі на службі в олігархів та політиків. URL: https://www.radiosvoboda.org/a/27042051.html (дата звернення: 15.03.2019).

[11] «Надо вернуть Турции»: РоссСМИ распространили фейк о позиции Эрдогана по Крыму. URL: https://bykvu.com/ru/bukvy/treba-povernuti-turechchini-roszmi-rozpovsjudili-fejk-shhodo-pozicii-erdogana-po-krimu/ (дата звернення: 07.11.2020).

[12] Yurkova O. Six Fake News Techniques and Simple Tools to Vet Them. URL: https://gijn.org/six-fake-news-techniques-and-simple-tools-to-vet-them/ (дата звернення: 08.04.2019).

1. Маніпуляції з медіаданими:

- редагування;
- подання справжніх медіаданих в іншому контексті, зміна часу і місця їх створення;
- створення повністю недостовірного медіаконтенту.

2. Маніпулювання новинами:

- викривлення сенсу заголовків новин;
- подання окремої думки як факту;
- викривлення фактів;
- подання повністю недостовірної інформації як факту;
- ігнорування важливих деталей, які змінюють контекст.

3. Маніпулювання експертними оцінками:

- використання думок псевдоекспертів (несправжніх експертів, експертів в інших сферах тощо) та аналітичних центрів;
- перекручування заяв експертів або приписування видуманих заяв справжнім експертам;
- викривлення перекладу.

4. Маніпулювання повідомленнями:

- використання повідомлень маргінальних суб'єктів;
- перекручування реальних повідомлень з авторитетних джерел;
- посилання на неіснуючі повідомлення з авторитетних джерел.

5. Маніпуляції з результатами досліджень:

- використання слабкої або несправжньої методології;
- неправильна інтерпретація результатів;
- неправильні порівняння.

У цій же праці було розкрито методи та інструменти викриття подібного виду підробок.

Однією з основних ознак інформаційної атаки є різкий дисбаланс позитивних і негативних повідомлень у доборі матеріалів, відсутність коректного обговорення різних точок зору, коли витісняється раціональна складова й обговорення відбувається на рівні емоцій та особистих звинувачень[13].

Емоційна складова є характерною рисою інформаційно-психологічного впливу. Коли людина лякається, в неї перестають працювати аналітичні центри. Психовіруси розраховані на те, щоб викликати в людини паніку та страх шляхом спекуляції на базових потребах. Наприклад, панічні новини про те, що все «жахливо подорожчає», уводять особу у стан паніки, вона стає не в змозі нормально аналізувати дійсність. Коли людину «зомбують», регулярно підкидаючи їй певні ідеї, то вони приживаються як негласні аксіоми. Така людина буде вкрай важко сприймати будь-які нові ідеї, якщо вони входять у конфлікт з укоріненими старими[14].

- *У серпні-вересні 2008 року один з українських банків зазнав прицільної інформаційної атаки[15], у тому числі із застосуванням повідомлень в мережі «Інтернет». Ця атака тривала кілька тижнів та була спрямована на те, щоб спровокувати паніку серед вкладників, які б масово почали виводити з банку свої кошти. Такі зловмисні дії досягли запланованої мети. За короткий період часу тисячі вкладників забрали з банку декілька мільярдів доларів. У результаті Національний банк України був вимушений здійснити рефінансування цього банку на суму 5 млрд. грн. Генеральною прокуратурою України було порушено кримінальну справу за доведення установи до банкрутства за ознаками злочину, передбаченого ч. 3 ст. 15, ст. 219 Кримінального кодексу України. Описана ситуація в подальшому сприяла посиленню фінансової кризи в усій державі.*

[13] Пода Т. А. Інформаційна війна як стратегія формування політичної свідомості (соціально-філософський аналіз). *Вісник Національного авіаційного університету*. Сер.: Філософія. Культурологія. 2014. № 1. С. 69.

[14] Ющенко А. Г. Украина обязана выиграть информационную войну. *Україна третє тисячоліття*. 2014. № 3. С. 22.

[15] Жертва рейдеров. Хроника атаки на «Проминвестбанк». URL: https://minfin.com.ua/2008/10/17/pib/ (дата звернення: 07.11.2020).

ПРОПАГАНДА

Одним з інструментів інформаційного впливу є пропаганда. В. Яковлев[16] розрізняє такі її методи:

- *«гнилий оселедець»*. Використовується проти конкретної особи або групи осіб, стосовно яких висуваються неправдиві звинувачення, які мають бути якомога скандальнішими (розбещення дітей, убивство з корисливих мотивів тощо). Метою обвинувачення є виклик широкого обговорення несправедливості, неправдивості обвинувачення. Поступово згадування об'єкта у зв'язку зі скандалом наростає та немовби в'їдається в його одяг, залишаючи за ним шлейф «гнилого оселедця». Таким чином, під час згадування імені об'єкта він постійно асоціюється з брудним скандалом;
- *«перегорнута піраміда»* є прийомом створення текстів, коли пріоритетність інформації зменшується від початку тексту до його закінчення. Цим досягається приковування уваги до гучного початку матеріалу. Об'єкт впливу може не дочитувати матеріал до кінця, проте основний посил залишиться в його пам'яті;
- *«велика брехня»* полягає в тому, що аудиторії впевнено пропонується скомпонована та добре продумана велика брехня, здатна викликати емоційну травму. Це така глобальна та страшна брехня, коли практично неможливо повірити, що можна брехати про таке (наприклад, інформація про розп'ятого хлопчика);
- *«40 на 60»* полягає в донесенні інформації, в якій 60 % інформації дається на користь супротивника, а інші 40 % – на користь суб'єкта інформаційного впливу. Перша частина інформації спрямована на заслуговування довіри супротивника, друга – на донесення дезінформації;
- *«абсолютна очевидність»* спрямована на створення у групи людей ефекту приєднання. Інформація, яку планується впровадити в маси, не доказується, а позиціонується як очевидний факт, що підтримується більшістю людей. Незважаючи на свою простоту, цей метод є дуже ефективним, оскільки

[16] Яковлев В. «Гнилая селедка», «большая ложь», «40 на 60» – Владимир Яковлев о приемах пропаганды. URL: https://www.stopfake.org/gnilaya-seledka-bolshaya-lozh-40-na-60-vladimir-yakovlev-o-priemah-propagandy/ (дата звернення: 15.03.2019).

людська психіка автоматично реагує на думку більшості, намагаючись долучитися до неї. Більшість має бути переважаючою, а її підтримка абсолютною та безумовною, в іншому випадку ефект приєднання буде відсутнім.

Інформаційні ресурси з доброю репутацією подекуди самі можуть ставати інструментом маніпуляції. Особливо це актуально для тих ресурсів, які не проводять ретельний аналіз наданих їм даних на достовірність. Б. Буткевич[17] наводить таку схему: через спеціально створений ресурс запускається недостовірна інформація цю інформацію без перевірки публікують інші засоби масової інформації та інформаційні ресурси країни, ЗМІ іншої країни, зацікавленої у проведенні інформаційної операції, викривають представлену інформацію як недостовірну, тим самим формуючи суспільну думку як у своїй країні, так і в державі – цілі проведення інформаційної операції.

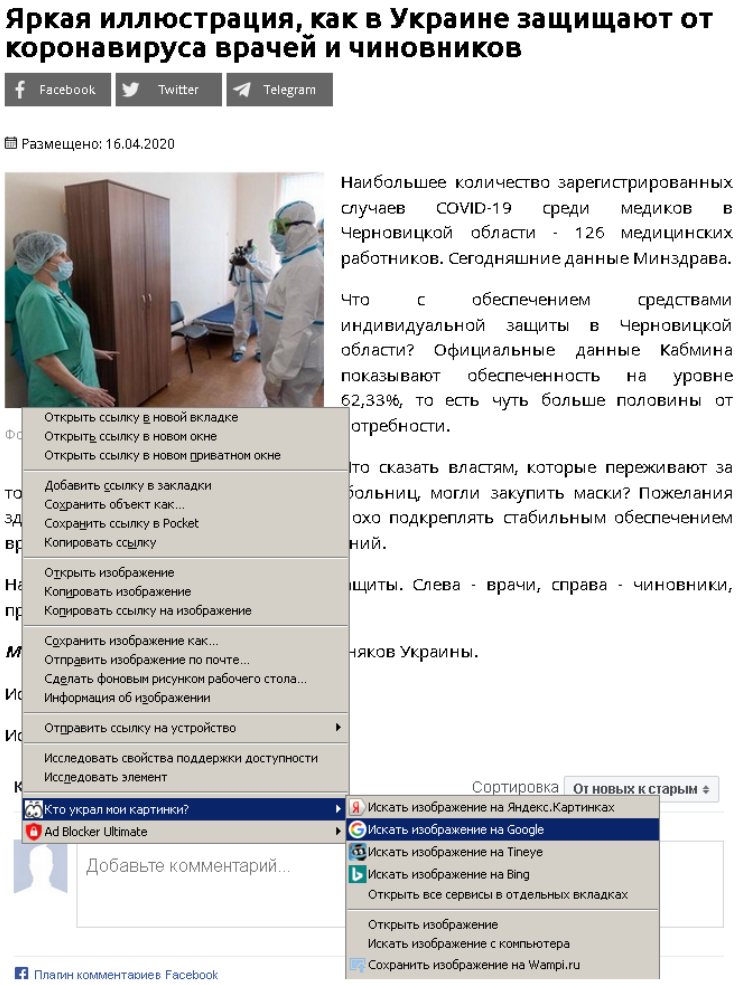
ЗАХОДИ ПРОТИДІЇ

Існує низка способів протидії неправдивим повідомленням. Умовно їх можна розділити на *логічні, технічні* та *комбіновані*. Найбільш простими та дієвими логічними способами є такі:

- критичне осмислення будь-якої інформації;
- під час сприйняття інформації потрібно намагатися більше керуватися розумом, аніж емоціями;
- звертати увагу на репутацію інформаційних ресурсів;
- перевіряти інформацію з декількох джерел;
- намагатися переглядати першоджерело відповідного інформаційного повідомлення.

Як приклад технічних інструментів викриття неправдивих фотоповідомлень можна навести плагін «Who stole my pictures» (зобр. 3), який легко знайти в мережі Інтернет та встановити у відповідному браузері.

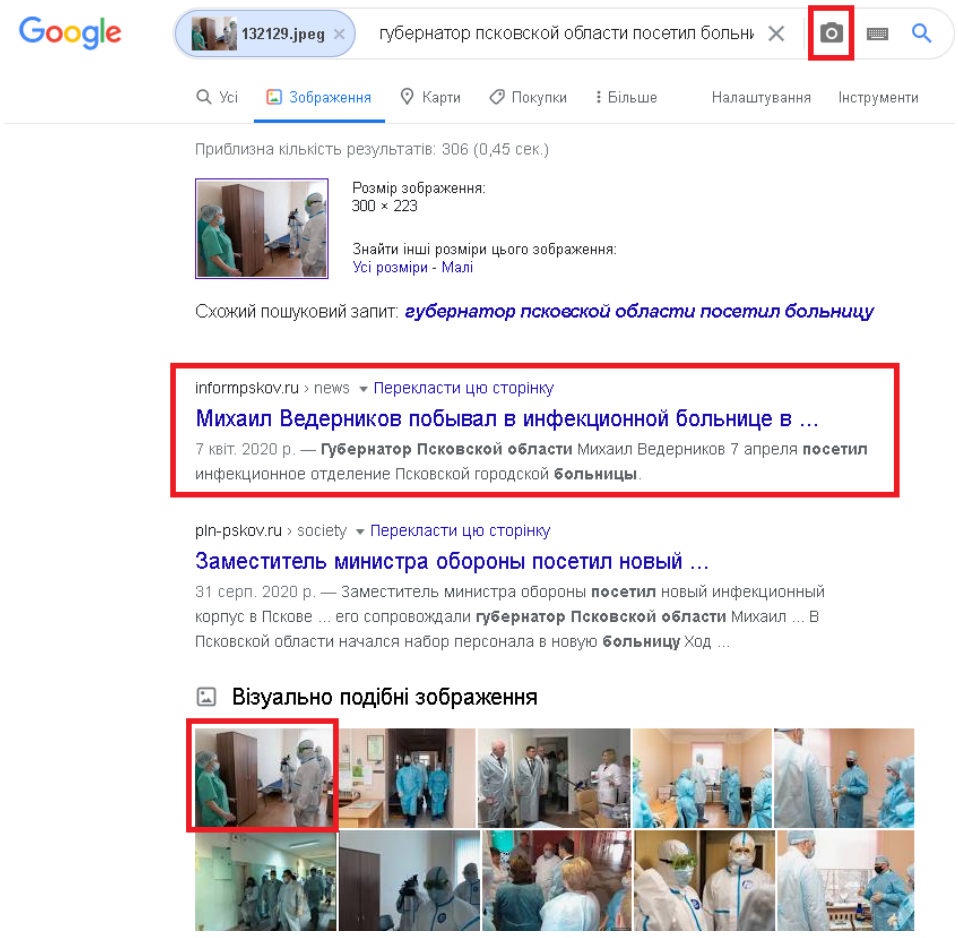
[17] Буткевич Б. Фабрика фейков. Какую угрозу несут сайты-паразиты. URL: https://vlada.io/articles/fabrika-feykov-kakuyu-ugrozu-nesut-saytyi-parazityi/ (дата звернення: 15.03.2019).



Зобр. 3. Використання інструменту пошуку зображень «Who stole my pictures»

Коментуючи новину на зобр. 3, потрібно відзначити, що вона була спрямована на маніпулювання громадською думкою (http://archive.is/tUogM). У ній коментується фотографія, яка нібито зроблена в українській лікарні, у той час як насправді зображення запозичено із новини про відвідування лікарні губернатором Псковської області в Російській Федерації (зобр. 4).

Для пошуку зображень в мережі «Інтернет» також згодиться і простий реверс-пошук за зображенням у пошуковій системі (зобр. 4).

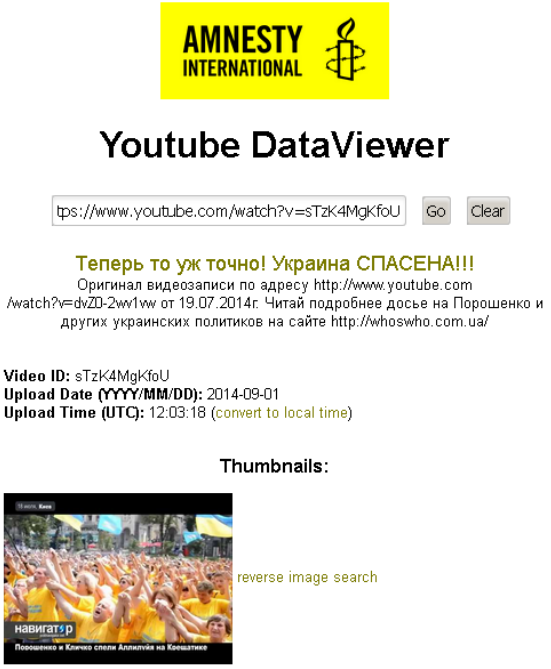


Зобр. 4. Використання зворотного пошуку за зображенням у пошуковій системі Google здійснюється шляхом натискання на зображення фотокамери на сторінці пошукової системи.

Крім наведених інструментів, для виявлення редагування зображень та аналізу додаткових даних можна використовувати такі сервіси як www.imageforensic.org та fotoforensics.com. Наприклад, вид аналізу Error Level Analysis або ELA дозволяє виявити накладені зображення, оскільки вони різняться за рівнем шуму – яскравістю точок (зобр. 5).

Зобр. 5. На рисунку видно, що рівень шуму для білого фону різко відрізняється від загального, це свідчить про те, що білий фон було створено окремо від основного фото (fotoforensics.com/tutorial-ela.php)

Для аналізу відефайлів, розміщених в мережі Youtube, може бути використаний сервіс citizenevidence.amnestyusa.org (зобр. 5).

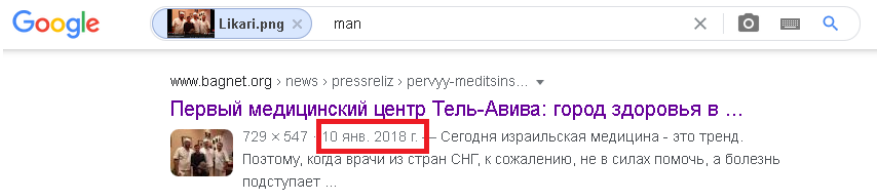


Зобр. 5. Аналіз фейкового відео, в якому опис не відповідає відеоряду

- *У листопаді 2020 року блогер А. Шарій випустив відеоролік, у якому продемонстрував фотографію Президента України з лікарями та вказав, що під час хвороби Президент нехтуючи масковим режимом фотографується з лікарями без маски (зобр. 6).*

Зобр. 6. Фрагмент відеоблога А. Шарія

Якщо з наведеного відеоряду зробити стопкадр з описаним фото, то під час подальшого зворотного пошуку в пошуковій системі легко встановити, що знімок було зроблено у 2016 році в Ізраїлі, про що йдеться, наприклад, у знайденій новині (зобр. 7) за адресою http://www.bagnet.org/news/pressreliz/353826/pervyy-meditsinskiy-tsentr-tel-aviva-gorod-zdorovya-v-gorode-mechty



Зобр. 7. Результати зворотного пошуку

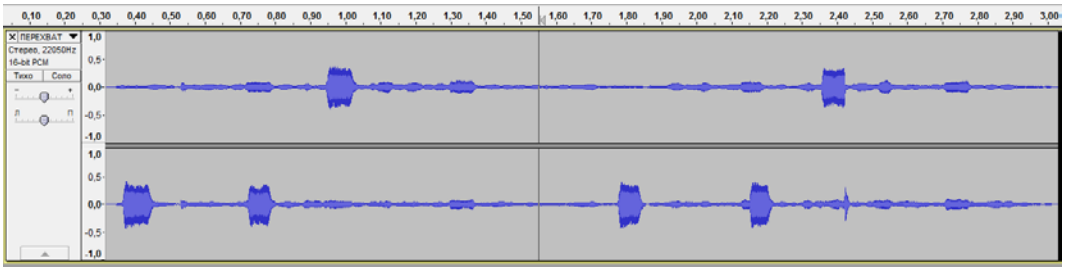
Наразі після публічного викриття А. Шарій перемонтував своє відео та видалив частину з описаним фото. Натомість видалений

фрагмент можна переглянути за посиланням https://censor.net/ru/photo_news/3230988/propagandist_shariyi_vydal_feyik_o_tom_chto_bolnoyi_koronavirusom_zelenskiyi_fotografiruetsya_s_vrachami [18]

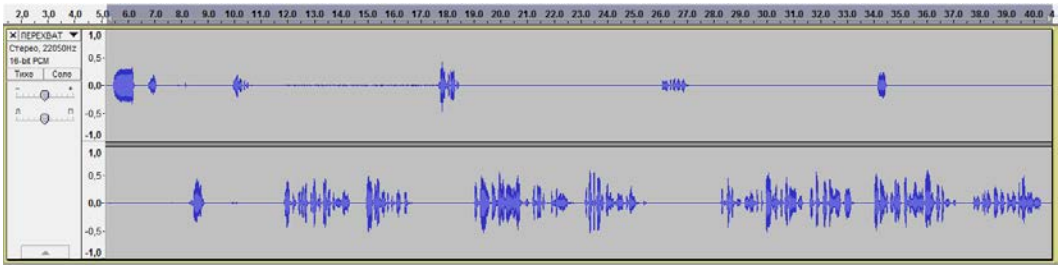
Коли мова йде про комбіновані способи виявлення фейків, то тут поєднуються обидва раніше наведених підходи. І це, насправді, найбільш ефективний інструмент протидії інформаційним загрозам.

- *27 березня 2014 року в мережі «Інтернет» за адресою https://www.youtube.com/watch?v=LTBpSGnD09I було розміщено аудіозапис із назвою «Телефонный разговор бойцов СОКОЛА. Следующая цель СБУ – ЯРОШ (18+) без цензури», в якому нібито два працівники спецпідрозділу міліції України обговорюють наказ свого керівництва про злочинну ліквідацію під час затримання одного відомого громадського і політичного діяча. Аналіз мови діалогу дозволяє зазначити, що один із співрозмовників має характерний російський говір, в який він зрідка вставляє українські слова, хоча для так званого українського суржику навпаки характерна вставка російських слів в українську мову. Аналіз сигналу запису в звуковому редакторі дозволив виявити факт того, що аудіосигнал нібито перехоплення телефонної розмови складається із двох незалежних сигналів для кожного співрозмовника. Тобто, запис учасників діалогу здійснювався із двох відокремлених незалежних мікрофонів, а потім два моносигнали було об'єднано у стереосигнал діалогу, що суперечить факту запису мовного сигналу із монофонічного телефонного каналу зв'язку. На зобр. 8 показано перші 3 секунди аудіозапису, де звучить дійсна стереофонічна музикальна заставка і в кожному каналі існують корельовані сигнали, а на зобр. 9 показаний наступний фрагмент некорельованих моносигналів, що об'єднанні у стереосигнал нібито перехвату із монофонічного телефонного каналу зв'язку.*

[18] Пропагандист Шарий выдал фейк о том, что больной коронавирусом Зеленский фотографируется с врачами, прикрепив фото 4-летней давности. ВИДЕО+ФОТО. URL: https://censor.net/ru/photo_news/3230988/propagandist_shariyi_vydal_feyik_o_tom_chto_bolnoyi_koronavirusom_zelenskiyi_fotografiruetsya_s_vrachami (дата звернення: 17.11.2020).



Зобр. 8. Перші 3 секунди аудіо запису, де звучить дійсна стереофонічна музикальна заставка і в кожному каналі існують корельовані сигнали.



Зобр. 9. Фрагмент аудіозапису некорельованих моносигналів, що об'єднані у стереосигнал нібито перехоплення із монофонічного телефонного каналу зв'язку[19]

Велику кількість інструментів розпізнавання фейків наведено на сайтах stopfake.org, snopes.com, factcheck.org, truthorfiction.com. Корисними також є розроблені для бізнесу рекомендації з протидії негативу в інформаційному просторі, які можуть бути адаптовані до більш широкого вжитку[20].

Найбільш складним і часовитратним, проте достатньо ефективним методом протидії неправдивим повідомленням, на нашу думку, є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій. Усе наведене дає підстави говорити про необхідність активізації в нашій країні зусиль з розбудови ефективної структури інформаційного протиборства.

[19] Носов В .В., Манжай О. В. Окремі аспекти протидії інформаційній війні в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. № 1(29). С. 26-29.

[20] Противодействие негативу в информационном пространстве: методические рекомендации / З. Чистяков, М. Шпаченко. Агентство конфликтного PR - /PR і Z/, 2012. 32 с.

МОДУЛЬ № 9:

ПРАВОВІ ЗАСАДИ КІБЕРГІГІЄНИ

МОДУЛЬ № 9: **ПРАВОВІ ЗАСАДИ КІБЕРГІГІЄНИ**

У контексті вивчення кібергігієни працівниками органів державної влади та місцевого самоврядування потрібно розуміти окремі аспекти вітчизняного законодавства, яке має давні традиції унормування правил безпечної роботи з інформацією.

У національних нормативно-правових актах на сьогодні відсутнє безпосереднє згадування такої категорії, як «кібергігієна». Водночас найбільш дотичними термінами у досліджуваному контексті є «інформаційна безпека» та «кібербезпека».

Згідно зі статтею 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу.

25 лютого 2016 р. Указом Президента України № 47/2017 було затверджено Доктрину інформаційної безпеки України, в якій зазначено, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Інформаційна безпека та кібербезпека держави є складовою частиною її національної безпеки. В Україні питанню забезпечення національної безпеки традиційно приділяють велику увагу. Здійснивши екскурс в історію, можна побачити, що від самого початку становлення України як незалежної держави методично ухвалювалися нормативно-правові акти, які містили безпосередні вказівки для того чи іншого напряму забезпечення національної безпеки.

У зв'язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України», який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектору безпеки України.

Відповідно до п. 9 ч. 1 ст. 1 цього Закону, ***національна безпека*** – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз.

Складові частини національної безпеки можна представити як на зобр. 1.

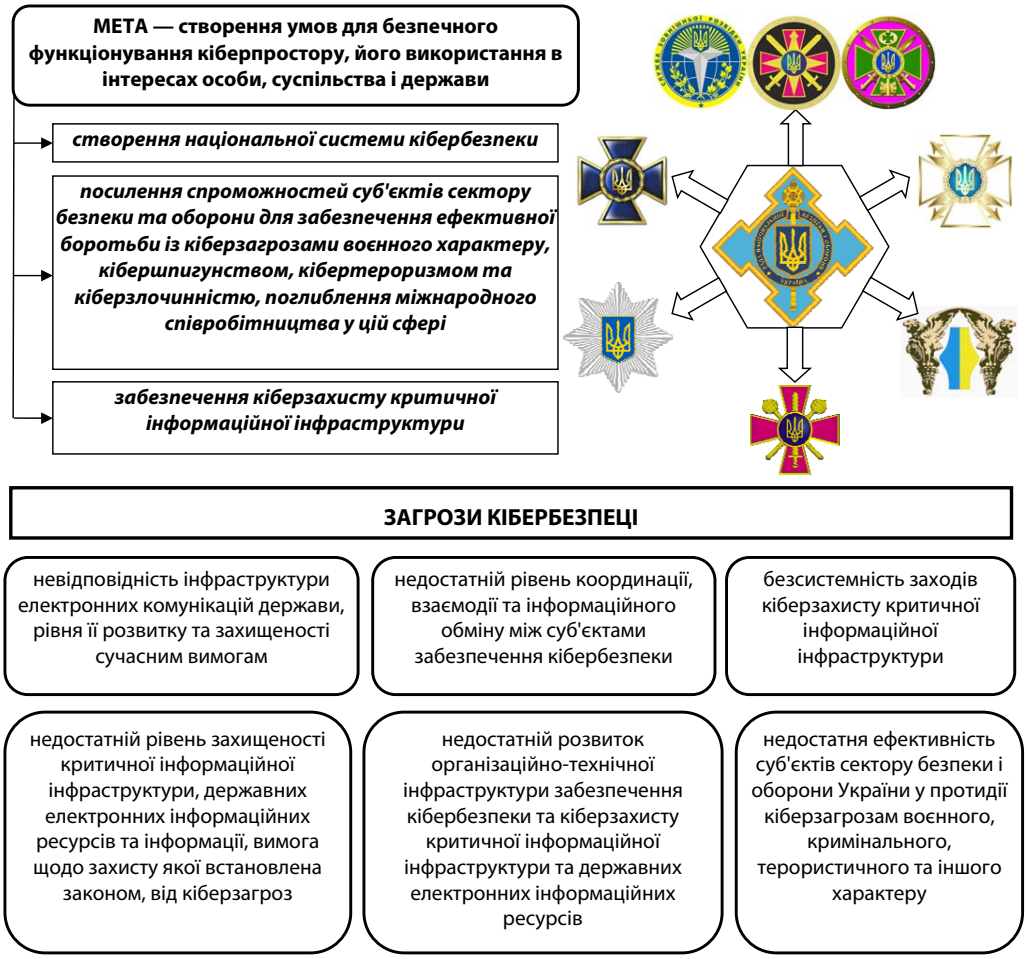
Зобр. 1. Структура національної безпеки України

За вказаними напрямами безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо.

Окремим нормативним актом затверджено ***Стратегію кібербезпеки України*** – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Докладніше структуру вказаного документа зображено на зобр. 2.

Слід наголосити, що в Законі України «Про національну безпеку України» не надається визначення термінів «інформаційна безпека» та «кібербезпека». На законодавчому рівні їх закріпили законами України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 та «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007.

Зокрема ***кібербезпека*** – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.



Зобр. 2. Основні елементи стратегії кібербезпеки України

Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

Кібергігієна є важливим елементом кібербезпеки, проте ці поняття не є тотожними. Якщо кібербезпека пов'язана з об'єктивним оцінюванням дій, спрямованих на підтримку безпеки та дотримання захисту від кібератак, то кібергігієна асоціюється зі знаннями про безпеку в інтернеті та правилами покращення кібербезпеки[21]. Також кібергігієна передбачає дотримання правил поведінки, що стосуються інформаційної безпеки.

Згідно з п. 13 розділу III Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки, під ***інформаційною безпекою*** розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

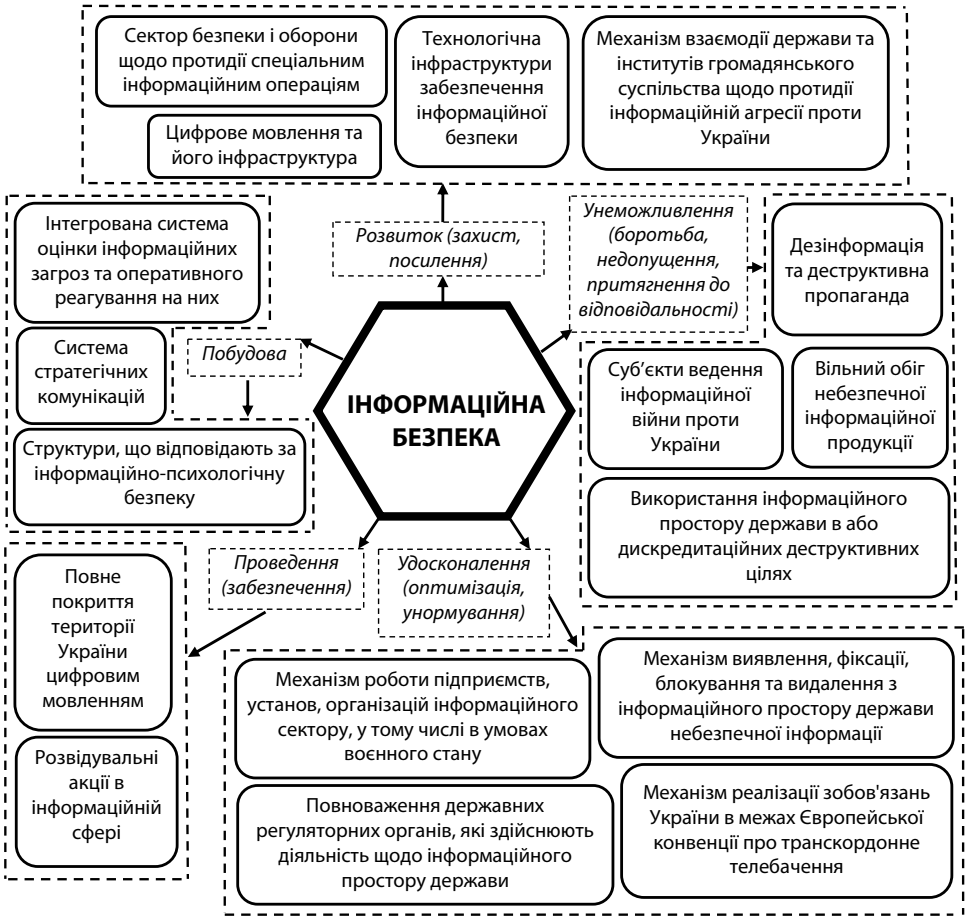
- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам і забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

[21] Neigel A. R., Claypoole V. L., Waldfogle G. E., Acharya S., Hancock G. M. Holistic Cyber Hygiene Education: Accounting for the Human Factors. *Computers & Security.* 2020. Vol. 92. 101731 (DOI: 10.1016/j.cose.2020.101731).

Виходячи зі змісту Доктрини інформаційної безпеки України, на зобр. 3 представлено основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки як складової частини національної безпеки України є:

- громадяни України та їх об'єднання;
- Верховна Рада України, яка серед іншого ухвалює закони у сфері інформаційної безпеки, визначаючи тим самим державну політику в цій сфері;
- Президент України, який забезпечує послідовне проведення державної інформаційної політики, інформаційний суверенітет та інформаційну безпеку України;
- Кабінет Міністрів України, який організовує діяльність виконавчої влади щодо забезпечення інформаційної безпеки;
- Рада національної безпеки і оборони України, яку очолює Президент України, координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки України;
- інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;
- засоби масової інформації та інші суб'єкти, які здійснюють інформаційну діяльність;
- наукові установи та навчальні заклади, які, серед іншого, проводять наукові дослідження та здійснюють підготовку фахівців з інформаційної безпеки.



Зобр. 3. Основні пріоритети забезпечення інформаційної безпеки

Залежно від конкретного виду інформації встановлюються різні рівні її захисту. Для визначення конкретних захисних механізмів використовується принцип поділу інформації за порядком доступу на відкриту та з обмеженим доступом. Загальна структура такого поділу наведена на зобр. 4.

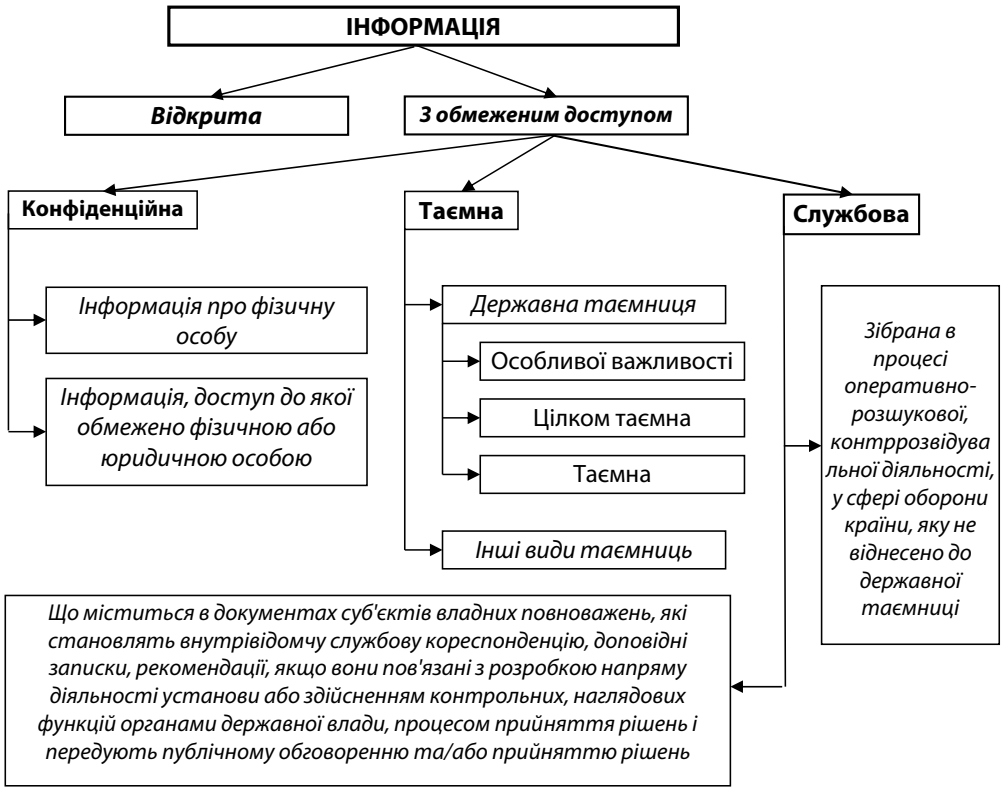
Захист відкритої інформації в державних органах регламентують:

1. Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 08.10.1997 № 1126[22].

[22] Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (дата звернення: 12.07.2017).

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373[23].

Захисту потребують такі властивості відкритої інформації, як *цілісність і доступність.*



Зобр. 4. Класифікація інформації за порядком доступу

Будь-яка інформація є **відкритою**, крім тієї, що віднесена законом до інформації з обмеженим доступом. До відкритої інформації, що підлягає захисту, відносять інформацію, яка належить до державних інформаційних ресурсів, а також про діяльність суб'єктів владних повноважень, військових формувань, яка

[23] Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стор. 164, стаття 878.

оприлюднюється в інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами.

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію»[24], ***конфіденційною*** є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи *у визначеному* нею *порядку* відповідно до *передбачених* нею *умов*, а також *в інших випадках, визначених законом*. Встановлення системи захисту є правом, а не обов'язком власника. Конфіденційна та службова інформація належать до інформації з обмеженим доступом, але не всяка інформація може бути визнана такою. Законодавець встановлює з цього приводу певні обмеження.

За розголошення конфіденційної інформації, що не є власністю держави, може наступати адміністративна відповідальність у порядку, визначеному ст. 164-3 Кодексу України про адміністративні правопорушення (КУпАП) від 07.12.1984. Крім того, адміністративна відповідальність може наставати також за порушення порядку використання конфіденційної інформації (ст. 186-3 КУпАП).

Більш урегульованими з правової точки зору є питання захисту службової інформації. Порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, детально прописаний у Типовій інструкції, затвердженій Постановою Кабінету Міністрів України від 19.10.2016 № 736[25].

За порушення роботи зі службовою інформацією передбачена адміністративна, а в окремих випадках – кримінальна відповідальність. Так, згідно зі ст. 212-5 КУпАП, порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів

[24] Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

[25] Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету міністрів України від 19.10.2016 № 736. *Офіційний вісник України*. 2016. № 85 (04.11.2016), стор. 102, стаття 2783.

громадян і на посадових осіб – від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян. Повторне вчинення правопорушення збільшує розмір штрафу.

Кримінальна відповідальність встановлюється за розголошення службової інформації (зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни) *нерезидентам* України (іноземним підприємствам, установам, організаціям або їх представникам) (ст. 330 Кримінального кодексу України).

Також належать до інформації з обмеженим доступом ***персональні дані*** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Наразі в Україні діє Закон України «Про захист персональних даних» від 01.06.2010, яким унормовано порядок роботи з інформацією, що містить персональні дані[26].

Таку інформацію можна поділити на:

- **загальну**, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого, відповідно до п. 3 ст. 296 Цивільного кодексу України, допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо);
- **вразливі персональні дані (конфіденційна інформація про особу)**, що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Також, згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону

[26] Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997, *до конфіденційної інформації про особу* належать, зокрема, свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).

У 2012 році Конституційний суд України додатково розтлумачив, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовій, інтимній, товариській, професійній, діловій та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їхньою згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини[27].

Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 № 373 та інших нормативних актів у сфері захисту інформації, **загальна інформація про особу**, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані** – як службова інформація відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації згідно з вимогами Закону України «Про захист персональних даних» від 01.06.2010.

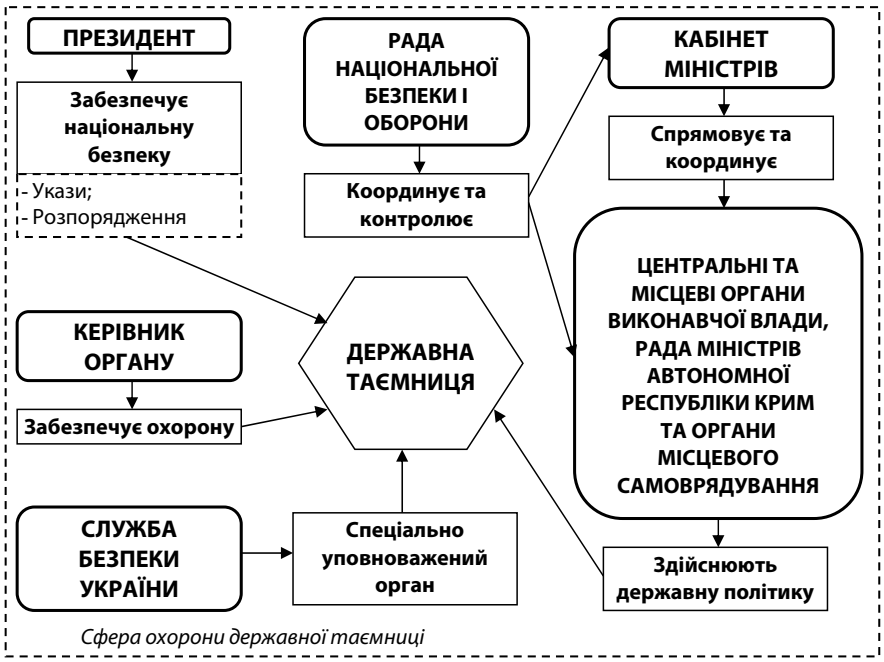
Захист інформації, яка становить державну таємницю, регламентується, перш за все, Конституцією України, кількома міжнародними договорами, ратифікованими

[27] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. *Офіційний вісник України*. 2012. № 9 (10.02.2012), стор. 106, стаття 332.

Верховною Радою України, Законом України «Про державну таємницю» від 21.01.1994[28], Кримінальним кодексом України та низкою підзаконних актів.

Згідно зі ст. 1 Закону України «Про державну таємницю», ***державна таємниця*** – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом, державною таємницею і підлягають охороні державою.

Організаційну структуру охорони державної таємниці умовно можна представити як на зобр. 5.



Зобр. 5. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

За порушення законодавства про державну таємницю передбачена дисциплінарна, адміністративна (ст. 212-2 КУпАП) та кримінальна відповідальність (ст. ст. 111, 114, 328, 329, 422 Кримінального кодексу України).

[28] Про державну таємницю: закон України від 21.01.1994; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1994. № 16 (19.04.1994). стор. 422. ст. 93.

ЧАСТИНА ІІ

ПРАКТИКУМ

ЗМІСТ

МОДУЛЬ № 1:

СОЦІАЛЬНА ІНЖЕНЕРІЯ

ПРАКТИЧНА ВПРАВА

«ЗАХИСТ ВІД ФІШІНГОВИХ АТАК»

Навчальна мета заняття: ознайомлення з принципами фішингових атак та протидії ним.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Фішінг (англ. *fishing* – рибна ловля) – одержання доступу до конфіденційних даних користувачів, яке досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Twitter, Instagram), банків (Приватбанк, Ощадбанк), інших сервісів (Google.com). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів тощо.

Фейк (Fake) – точна копія головної сторінки (або будь якої іншої сторінки) оригінального сайту, яка використовується для фішингу з метою отримання конфіденційних даних користувачів.

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти повідомлення, які надходять, та користуватись антифішінговими інструментами. Відповідні інструменти нерідко вбудовано у браузери.

1. Проаналізуйте продемонстровані тренером вебсторінки.

2. Визначте, які з них можуть бути фейками.

3. Обґрунтуйте свою відповідь.

ПРАКТИЧНА ВПРАВА

«АНАЛІЗ ПОШТОВОГО ПОВІДОМЛЕННЯ»

Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Фішінгові повідомлення часто надходять користувачам за допомогою електронної пошти.

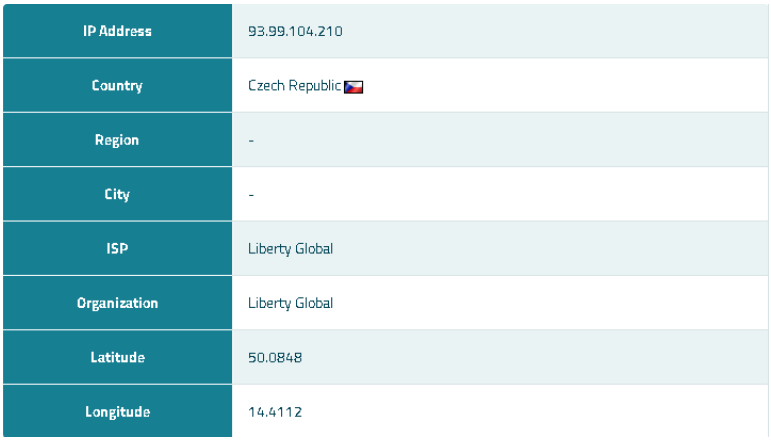
Змоделюємо ситуацію, яким чином це може відбуватися та як можна запобігти цьому негативному явищу.

Спершу слід зареєструвати тестову поштову скриньку, на яку будемо одержувати відповідні повідомлення. Для цього можна скористатися поштовим сервісом secmail.pro, реєстрація на якому доступна через мережу TOR. Враховуючи наведене, спершу потрібно встановити на комп'ютері TOR-браузер (https://www.torproject.org/ru/download/), після чого зареєструватися за адресою http://secmailw453j7piv.onion/ або http://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion/.

Після реєстрації електронної поштової скриньки тренер надішле на неї лист.

Для того, щоб виявити підробку в листі, потрібно дослідити його поштовий заголовок. Для цього слід після відкриття листа натиснути Options: View Full Header.

Заголовок електронного поштового листа можна дослідити або вручну, або за допомогою програм чи сервісів (зобр. 1.)



IP Address	93.99.104.210
Country	Czech Republic
Region	-
City	-
ISP	Liberty Global
Organization	Liberty Global
Latitude	50.0848
Longitude	14.4112

Зобр. 1. Результат аналізу заголовка поштового листа за допомогою сервісу iplocation.net

Виходячи з даних, наведених в теоретичних відомостях:

1. Зареєструвати поштову скриньку та надіслати тестове повідомлення.

2. Проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа за допомогою сервісів http://ua.smart-ip.net/trace-email, https://toolbox.googleapps.com/apps/messageheader/analyzeheader, або https://www.iplocation.net/trace-email.

▶ Приклад. «*Розшифровка типового заголовка листа*»

Return-path:* *@ukr.net** – *зворотна адреса, вказана відправником;*

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) – *лист отримано від хосту mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21;*

by mx5.mail.ru – *ім'я комп'ютера, який приймав повідомлення;*

with esmtp id 1COlNS-000F0L-00 – *комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COlNS-000F0L-00;*

Tue, 18 Nov 2008 02:14:18 +0300 – *передавання листа здійснювалося у вівторок, 18 листопада 2008 року о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 – *отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й*

«заборонену» відносно домену одержувача чи відправника. В цьому випадку, поштовий сервер-одержувач mx5.mail.ru здійснив SPF-запит до домену ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домену ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домену ukr.net);

envelope-from=*@ukr.net*** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 «HELO copm1» ident: «NO-IDENT-SERVICE[2]» whoson: «s-m-i-t»);

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others);

Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист;*

Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*

From: *@ukr.net*** *– напис на «конверті», від кого лист;*

To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net*** *– адреси доставки листа;*

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (у разі заміни кодування тема матиме вигляд напису «Предложение»);*

Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим 2-м часовим поясом);*

MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено цей лист;*

Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема, встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*

boundary=»----=_NextPart_000_0015_01C4C076.3170DA90» *– стандартизація розбивання великих листів на декілька частин. У полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок – унікальний обмежувач фрагментів «boundary=<boundary string>». А потім перед кожним фрагментом пишеться цей рядок з двома мінусами попереду, а в кінці фрагментації – ще один рядок, який завершується такими ж двома мінусами.*

X-Priority: 3 *– пріоритет листа, позначений цифрами.*

X-MSMail-Priority *– нестандартне поле Microsoft – пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай використовуються*

слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму виробника програмного забезпечення;*

X-Spam: Not detected *– лист не визначено як спам.*

МОДУЛЬ № 2:

БЕЗПЕЧНЕ КОРИСТУВАННЯ МЕРЕЖЕЮ «ІНТЕРНЕТ»

ПРАКТИЧНА ВПРАВА

«БЕЗПЕЧНИЙ ПЕРЕГЛЯД ВЕБСТОРІНОК»

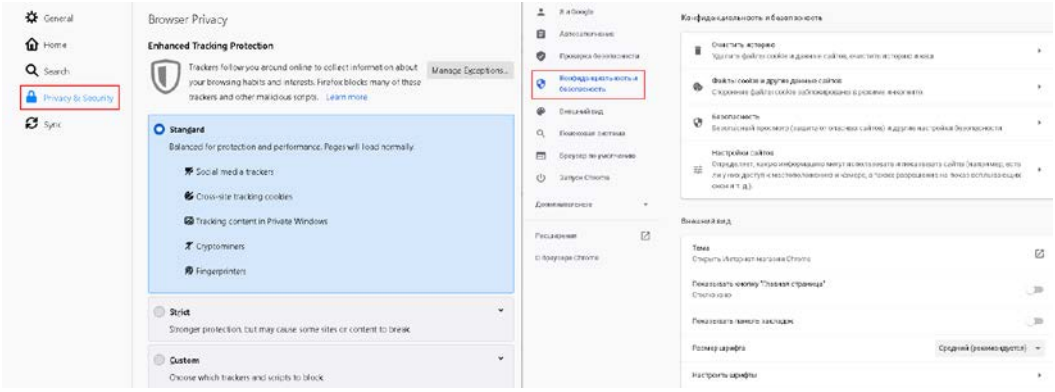
Навчальна мета заняття: здійснити налаштування браузеру та встановлення додаткових плагінів для безпечного серфінгу в мережі.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено.**

Перегляд вебсторінок, як правило, здійснюється за допомогою програм-браузерів, найпоширенішими серед яких є Chrome та Firefox. В усіх сучасних браузерах присутнє меню налаштувань, за допомогою якого можна здійснити налаштування безпеки та конфіденційності (зобр. 1).



Зобр. 1. Зліва направо налаштування безпеки у браузерах Firefox та Chrome

Якщо налаштування безпеки не повною мірою влаштовують користувача можна встановити додаткові плагіни. У якості плагінів за напрямом безпеки можна навести:

- AdBlock для блокування спливаючих вікон (https://adblockplus.org/ru/download);

- RequestPolicy для блокування міжсайтових запитів (https://www.requestpolicy.com/);
- HideMyBack для приховування або зміни певної інформації про ідентифікатори програм і пристроїв (https://chrome.google.com/webstore/detail/hide-my-back/adkllkhpobbaieagddmffnfkgibplegi);
- Click&Clean для видалення тимчасових файлів у браузері (https://www.hotcleaner.com/).

1. Налаштуйте параметри безпеки та конфіденційності браузера. Поясніть свій вибір налаштувань.

2. Встановіть додаткові плагіни, описані в матеріалах до заняття. Опишіть порядок їх використання.

ПРАКТИЧНА ВПРАВА

«СПОСОБИ ОРГАНІЗАЦІЇ БЕЗПЕЧНОГО З'ЄДНАННЯ В МЕРЕЖІ»

Навчальна мета заняття: відпрацювати різні технології забезпечення з'єднання в мережі.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Вхідні дані.

Перелік VPN-сервісів та проксі-серверів:

free-proxy.cz

vpnbook.com

protonvpn.com

Для налагодження безпечного з'єднання з віддаленими ресурсами може бути застосовано проміжні убезпечуючі механізми, як-от: проміжні проксі- або VPN-сервери. Для демонстрації роботи таких серверів можна здійснити таке.

Проксі-сервери

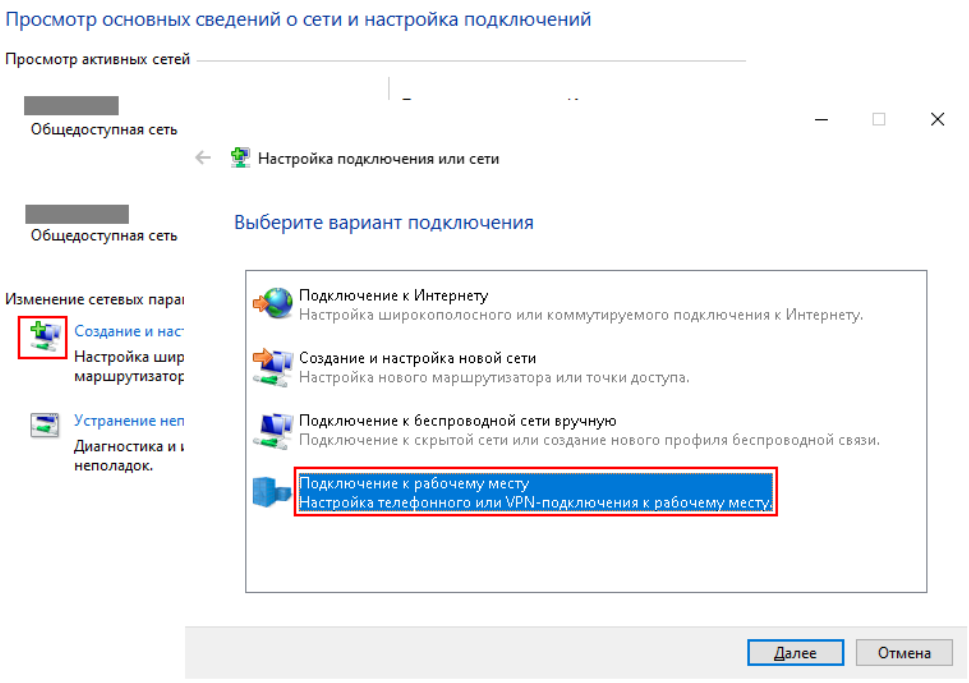
Відкрити сторінку http://free-proxy.cz/en/web-proxylist/, після чого обрати будь-який проксі-вебсервер. Ввести у відповідному вікні адресу 2ip.ua. Оцінити одержані результати (зобр. 1).

Зобр. 1. Результат використання проксі-серверу

VPN-сервери

На відміну від проксі-серверів, які працюють за окремими портами, VPN-сервери надають можливість організації повноцінного захищеного з'єднання між користувачем та відповідними ресурсами. Для користування VPN-сервером потрібно знати його налаштування та відповідні автентифікаційні дані.

Як правило, налаштувати відповідне підключення можна без необхідності встановлення додаткового програмного забезпечення. Для цього, наприклад, у системі Windows 10 слід відкрити «Центр управління мережами та спільним доступом» та створити нове з'єднання (зобр. 2).

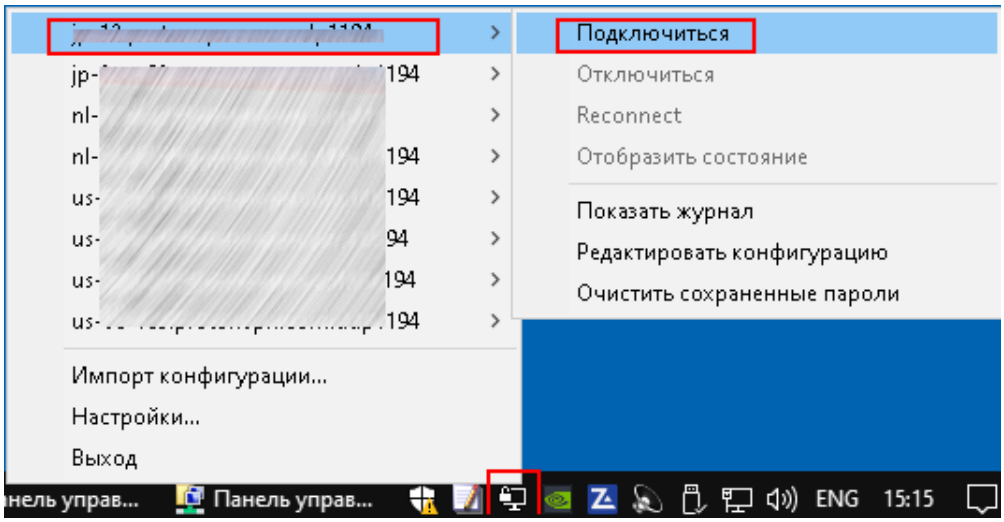


Зобр. 2. Налаштування нового з'єднання в операційній системі

Далі слід вказати адресу VPN-сервера та перейти у розділ «Зміна параметрів адаптера» та двічі натиснути на новоутвореному з'єднанні. Після цього слід ввести відповідне ім'я користувача і пароль та дочекатися з'єднання.

Більш універсальний спосіб налаштування VPN-з'єднання полягає у використанні спеціальних програм для організації такої діяльності. З цією метою може бути використано, наприклад, безкоштовний застосунок OpenVPN, який можна завантажити за адресою: https://openvpn.net/community-downloads/.

Після встановлення програми відповідні файли налаштування з'єднання записуються у папку Config програми OpenVPN. Запустивши програму слід обрати відповідну конфігурацію та під'єднатися до VPN-сервера (зобр. 3)



Зобр. 3. З'єднання з VPN-сервером за допомогою програми OpenVPN

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.

2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережного підключення операційної системи та 2) за допомогою VPN Client).

3. Переконатися у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом 2ip.ua).

4. Встановити Firewall та антивірус ZoneAlarm.

ПРАКТИЧНА ВПРАВА

«НАКЛАДАННЯ ЕЛЕКТРОННОГО ПІДПИСУ»

Навчальна мета заняття: відпрацювати різні технології забезпечення з'єднання в мережі.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

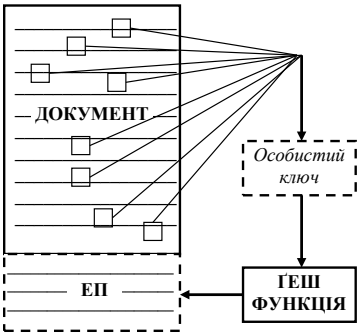
Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

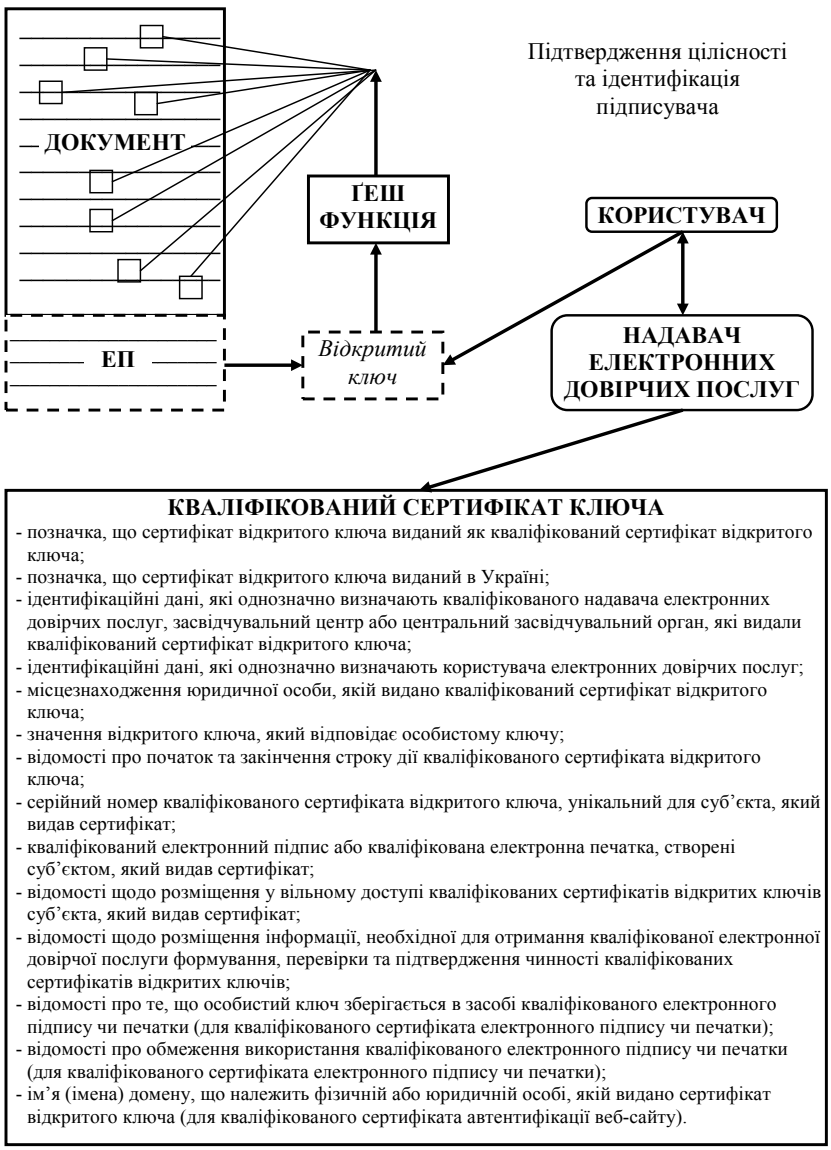
Реквізитом електронного документа є ***електронний підпис*** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис. Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа*.

Отже, ***особистий ключ*** – це параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів, а ***відкритий ключ*** – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Загальна схема накладання електронного підпису наведена на зобр. 1, а його перевірки – на зобр. 2.



Зобр. 1. Приблизна модель накладання електронного підпису



Зобр. 2. Приблизна модель перевірки електронного підпису

Накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується**, але при цьому можна впевнитись у *цілісності* документа й *ідентифікувати його підписувача*.

Одним із швидких способів організації роботи з електронним підписом є використання у зв'язці електронного підпису від Приватбанку та програми ІІТ Користувач ЦСК-1.

Відповідний алгоритм можна описати таким чином:

1. Завантажити програму ІІТ Користувач ЦСК-1 (http://acskidd.gov.ua/korustyvach_csk) та встановити її на комп'ютері.
2. Авторизуватись в системі Приват24 та в меню Усі послуги → Бізнес → Електронний цифровий підпис → Завантажити сертифікат згенерувати відповідні файли, потрібні для безпечного електронного документообігу. При виконанні цього завдання може знадобитися встановлення додаткових плагінів для браузера Google Chrome. Завантажити відповідні сертифіката можна за адресою https://acsk.privatbank.ua/certs.
3. Імпортувати заванатажені сертифікати до програми ІІТ Користувач ЦСК-1 через відповідне меню Параметри.
4. Після вчинення відповідних дій у програмі ІІТ Користувач ЦСК-1 можна підписувати різні документи, перевіряти вже наявні підписані файли на предмет автентичності електронного підпису та цілісності документа, виконувати функції шифрування / розшифрування документів.
5. У разі відсутності потреби у використанні електронного підпису, можна відкликати сертифікат на сторінці https://acsk.privatbank.ua/service.

Порядок проведення заняття

1. Завдання: одержати ключі електронного підпису через електронний кабінет у банку.
2. З використанням ресурсу ca.informjust.ua/sign накласти електронний підпис на довільний файл трьома способами. За допомого сервісу informjust.ua/verify перевірити цілісність документа. Змінити підписаний файл. Провести повторну перевірку.
3. З використанням електронного підпису авторизуватись в онлайн-будинку юстиції (online.minjust.gov.ua/login). Одержати інформацію з державного реєстру речових прав.
4. З використанням електронного підпису авторизуватися на порталі електронних послуг пенсійного фонду (portal.pfu.gov.ua). Перевірити відомості про свої відрахування.
5. З використанням електронного підпису авторизуватися в електронному кабінеті на порталі Державної фіскальної служби України (cabinet.sfs.gov.ua). Перевірити відомості про свої доходи.
6. Відпрацювати роботу програми «ІІТ Користувач ЦСК-1» за адресою: acskidd.gov.ua/korustyvach_csk.

МОДУЛЬ № 3:

БЕЗПЕЧНЕ КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

ПРАКТИЧНА ВПРАВА

«ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ПОШТОВОГО ОБЛІКОВОГО ЗАПИСУ»

Навчальна мета заняття: відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», смартфони або телефони у слухачів, флеш-накопичувачі за кількістю слухачів.

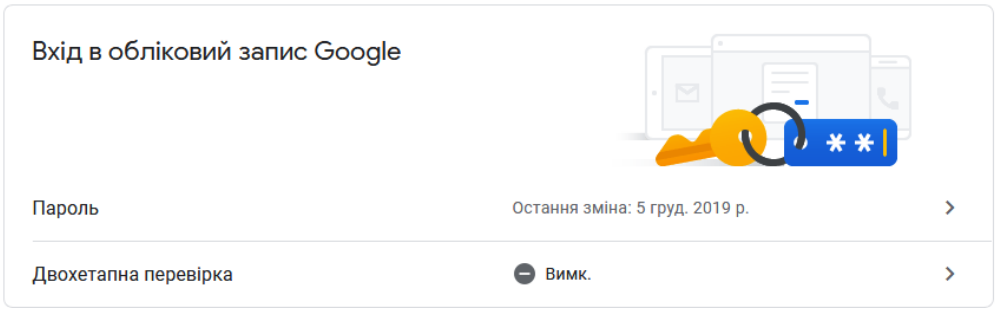
Порядок проведення заняття

Створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com.

Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.

Для облікового запису gmail.com

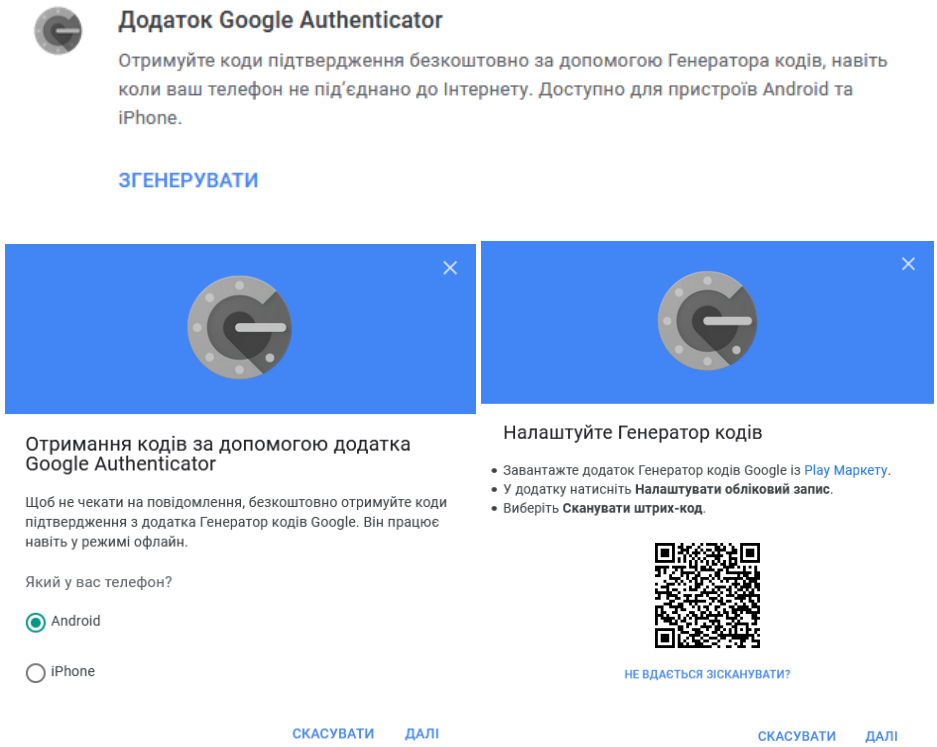
Перейти у розділ «Ваш обліковий запис» – «Безпека» – «Вхід в обліковий запис Google». Обрати «Двохетапна перевірка» – «Розпочати» (зобр. 1).



Зобр. 1. Розділ налаштувань двоетапної перевірки

Обрати автентифікацію через коротке текстове повідомлення і зареєструвати особистий телефон через отримання коду в sms і вводу його у відповідному полі налаштувань.

Знову увійти в «Безпека» – «Вхід в обліковий запис Google» – «Двоетапна перевірка» – «Розпочати» та додати інші варіанти другого етапу перевірки, щоб підтверджувати свою особу, а саме «Додаток Google Authenticator». Завантажити за наданим посиланням у смартфон додаток «Генератор кодів Google» (зобр. 2) та дотримуйтесь інструкцій щодо його налаштування.

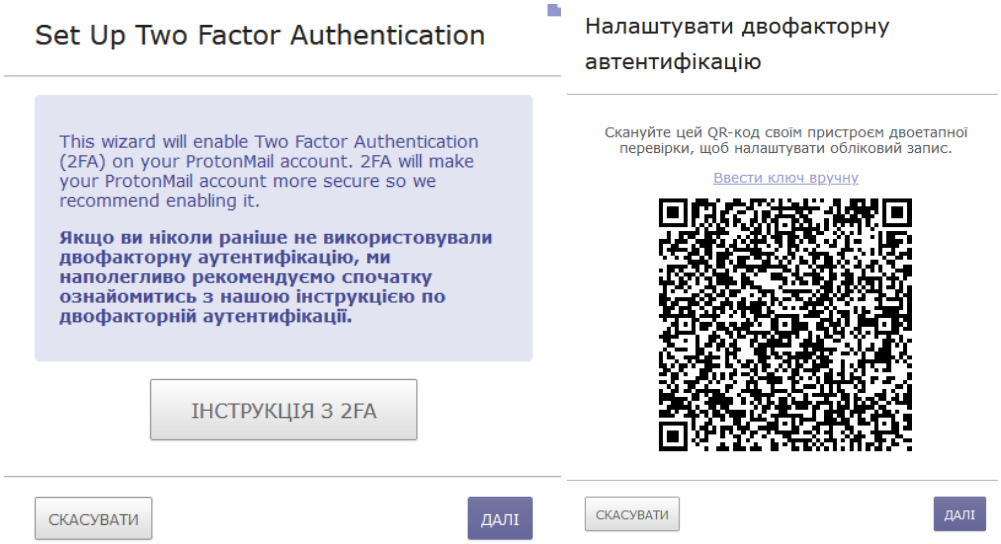


Зобр. 2. Інструкції майстру налаштувань Google Authenticator

Після закінчення налаштувань вийти із облікового запису та пройти вже двоетапну автентифікацію.

Для облікового запису protonmail.com

У поштовому обліковому записі protonmail перейти у розділ «Налаштування» – «Безпека» – «Увімкнути двоетапну перевірку» – «Налаштувати двофакторну автентифікацію» (зобр. 3).



Зобр. 3. Інструкції майстра налаштувань двофакторної автентифікації

Скористатися вже встановленим у смартфоні застосунком Google Authenticator (встановлюється з Google Play або App Store) і налаштувати двоетапну автентифікацію. Вийти із облікового запису та пройти вже двоетапну автентифікацію.

ПРАКТИЧНА ВПРАВА
«ПАРОЛЬНИЙ МЕНЕДЖЕР»

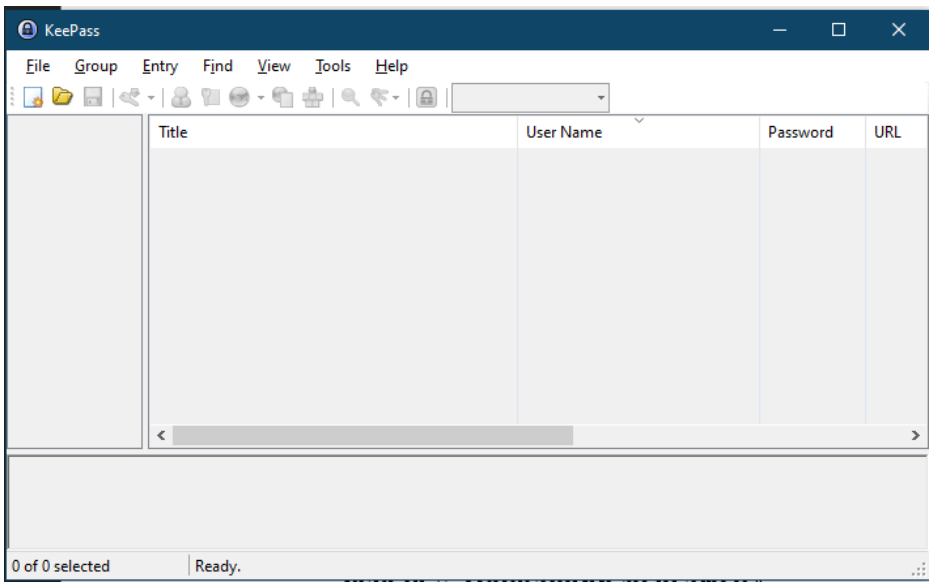
Навчальна мета заняття: встановити, налаштувати та опановувати використання парольного менеджера KeePass.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», смартфони або телефони у слухачів, флеш-накопичувачі за кількістю слухачів.

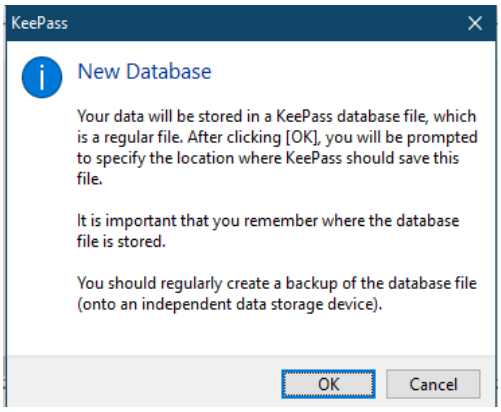
Порядок проведення заняття

Завантажити (https://keepass.info/index.html), встановити та запустити парольний менеджер KeePass Password Safe (зобр. 1).



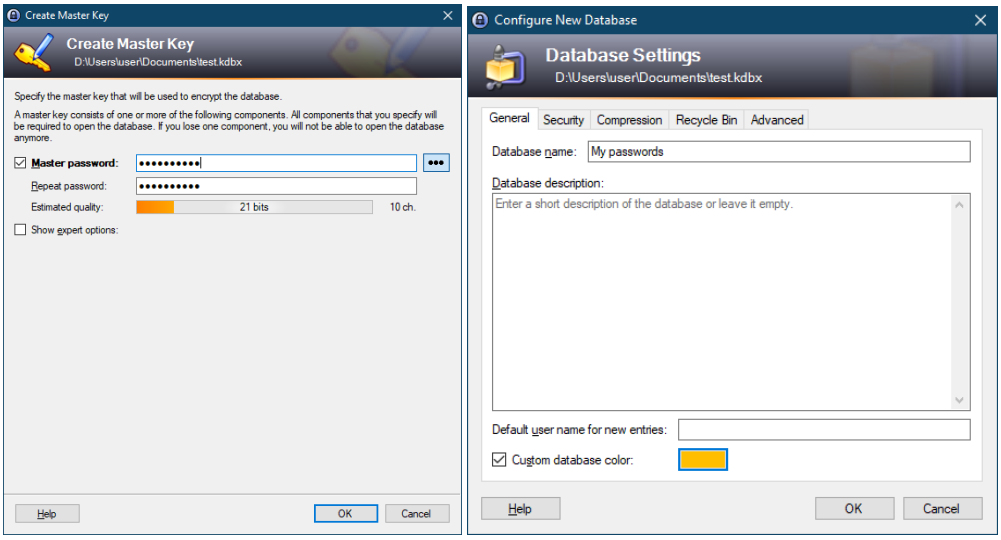
Зобр. 1. Головне вікно KeePass

Комбінацією клавіш (Ctrl+N) створити та вказати місце зберігання файлу нової бази паролів (зобр. 2).

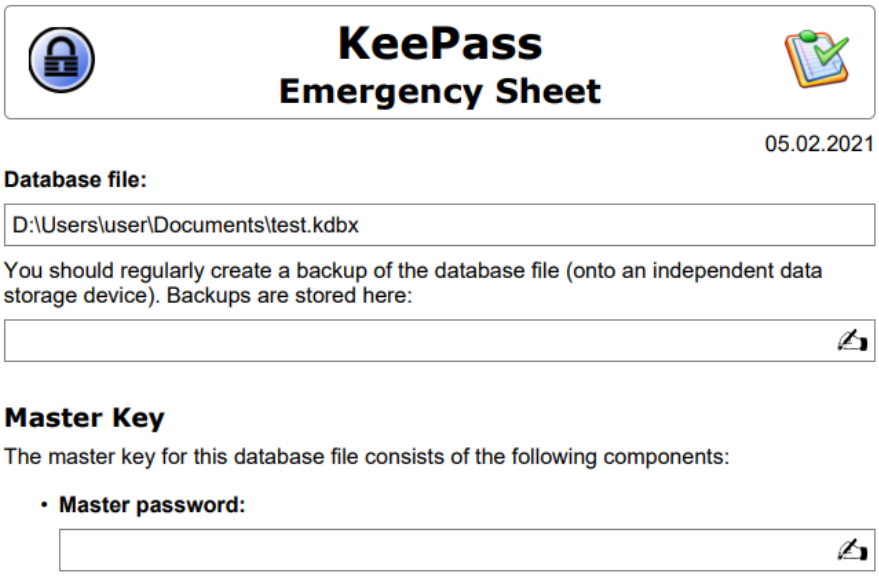


Зобр. 2. Повідомлення щодо створення нової бази паролів

Придумати та запам'ятати майстер-пароль (парольну фразу) довжиною не менше 10-ти символів із використанням маленьких та великих літер, цифр та спеціальних символів. Ввести майстер-пароль (парольну фразу) та вибрати ім'я для бази паролів (зобр. 3). Додатково можна роздрукувати основні дані щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля (зобр. 4).



Зобр. 3. Створення майстер-паролю та налаштування бази


KeePass
Emergency Sheet

05.02.2021

Database file:

D:\Users\user\Documents\test.kdbx

You should regularly create a backup of the database file (onto an independent data storage device). Backups are stored here:

Master Key

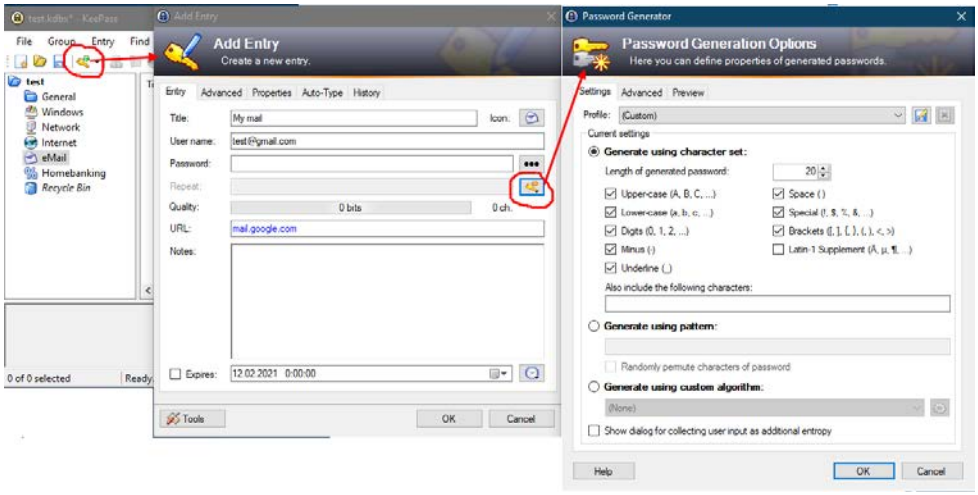
The master key for this database file consists of the following components:

- **Master password:**

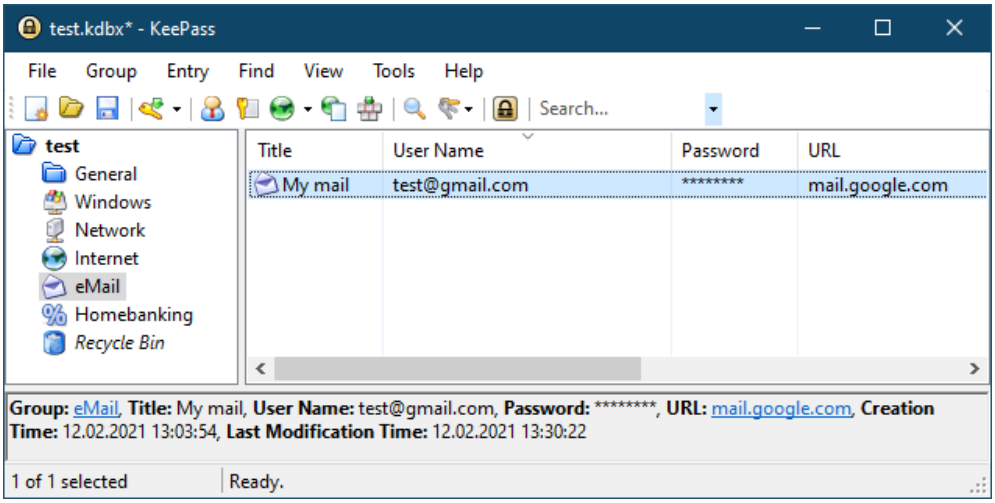
Зобр. 4. Пам'ятка щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля

В основному вікні KeePass зліва обрати теку «eMail», створити новий запис (комбінація клавіш Ctrl+I), заповнити поля для свого поштового облікового запису, перейти у налаштування Генератора паролів і обрати довжину пароля та абетку символів, з яких буде генеруватися пароль (зобр. 5). Завершити редагування, зберегти зміни (комбінація клавіш Ctrl+S) і переглянути створений запис (зобр. 6).

Зверніть увагу, що деякі вебсервіси забороняють наявність в паролі спеціальних символів. У такому випадку, або після генерації паролю вручну видалити спеціальні символи або виключити їх із абетки налаштувань Генератора паролів.



Зобр. 5. Створення і налаштування параметрів нового запису у базі паролів



Зобр. 6. Створений запис у базі паролів

Пройти автентифікацію в поштовому сервісі, використовуючи менеджер паролів. Для цього в KeePass обирається відповідний запис та почергово копіюється у буфер логін (комбінація клавіш Ctrl+B) та пароль (комбінація клавіш Ctrl+C), які почергово вставляються у відповідні поля форми автентифікації поштового сервісу.

ПРАКТИЧНА ВПРАВА

«ПЕРЕВІРКА ФАКТУ КОМПРОМЕТАЦІЇ ПОШТОВОЇ АДРЕСИ»

Навчальна мета заняття: пересвідчитись у відсутності або наявності витоку власних автентифікаційних даних.

Час проведення: 0,25 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

За адресами https://haveibeenpwned.com, https://monitor.firefox.com перевірити наявність власних поштових облікових записів у «зливах», де фігурують вкрадені дані автентифікації. У випадку знаходження поштових облікових записів у «зливах» терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію.

ПРАКТИЧНА ВПРАВА

«ЕЛЕКТРОННИЙ ПІДПИС ТА ШИФРУВАННЯ ПОВІДОМЛЕНЬ»

Навчальна мета заняття: налаштувати утиліту gpg4usb, створити повідомлення для співрозмовника, підписати та зашифрувати повідомлення. Співрозмовнику розшифрувати і перевірити підпис у отриманому повідомленні.

Час проведення: 1,75 год. Місце проведення: комп'ютерний клас.

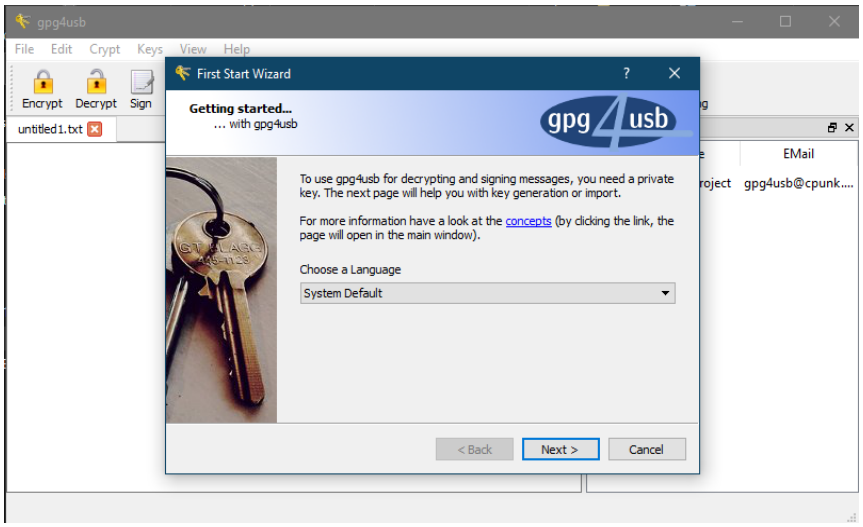
Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

Виконати такі дії:

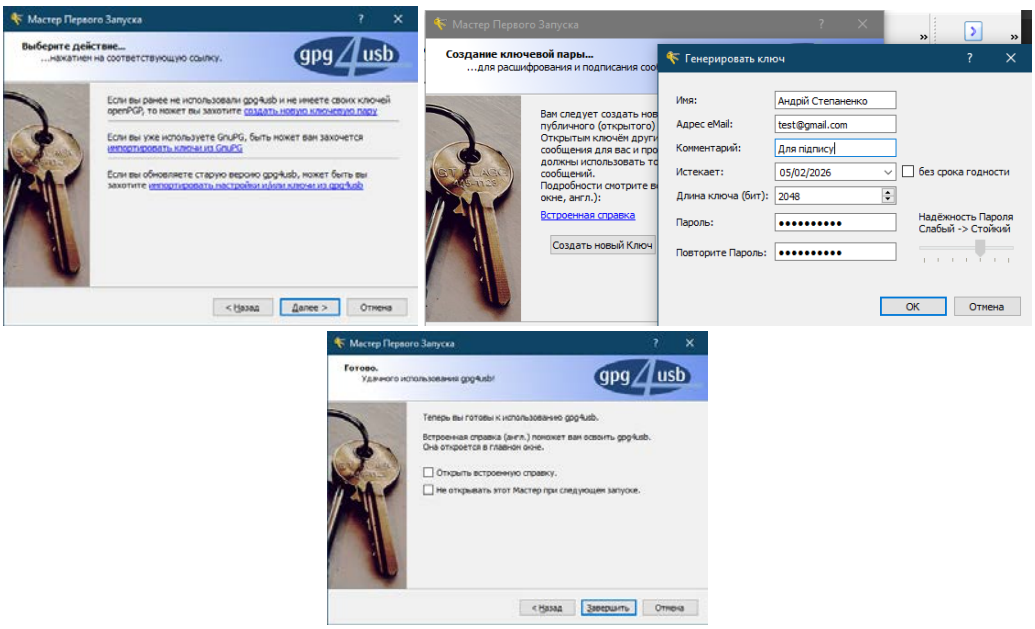
- встановити на свій флеш-накопичувач утиліту **gpg4usb**;
- згенерувати пару своїх ключів;
- експортувати свій публічний ключ в окремий файл *_pub.asc;
- обмінятися своїм публічним ключем з іншими;
- імпортувати у програму публічні ключі інших;
- створити повідомлення для співрозмовника, підписати повідомлення та зашифрувати його з використанням публічного ключа адресата;
- отримати підписане та зашифроване повідомлення, розшифрувати повідомлення та перевірити електронний підпис.

За посиланням https://www.gpg4usb.org/download.html вибрати та завантажити на особистий флеш-накопичувач архів утиліти gpg4usb. Розпакувати архів, запустити утиліту start_windows.exe та обрати зручну мову інтерфейсу (зобр. 1).



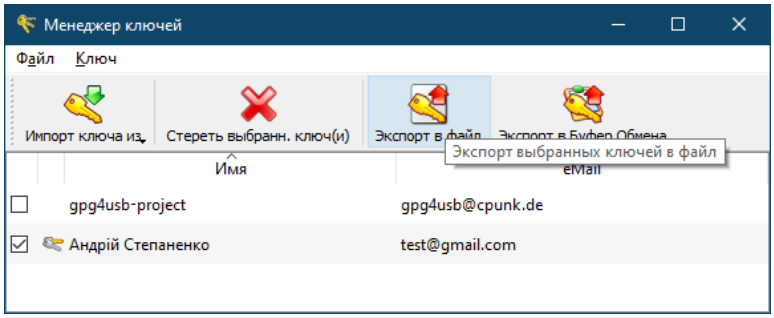
Зобр. 1. Налаштування мови інтерфейсу gpg4usb

Далі клікнути на посилання «Створити нову ключову пару», обрати «Створити новий Ключ» та заповнити відповідні поля персональними даними (пароль згенерувати та зберегти у менеджері паролів). Завершити налаштування у майстрі першого запуску (зобр. 2).



Зобр. 2. Генерування ключів у майстрі першого запуску

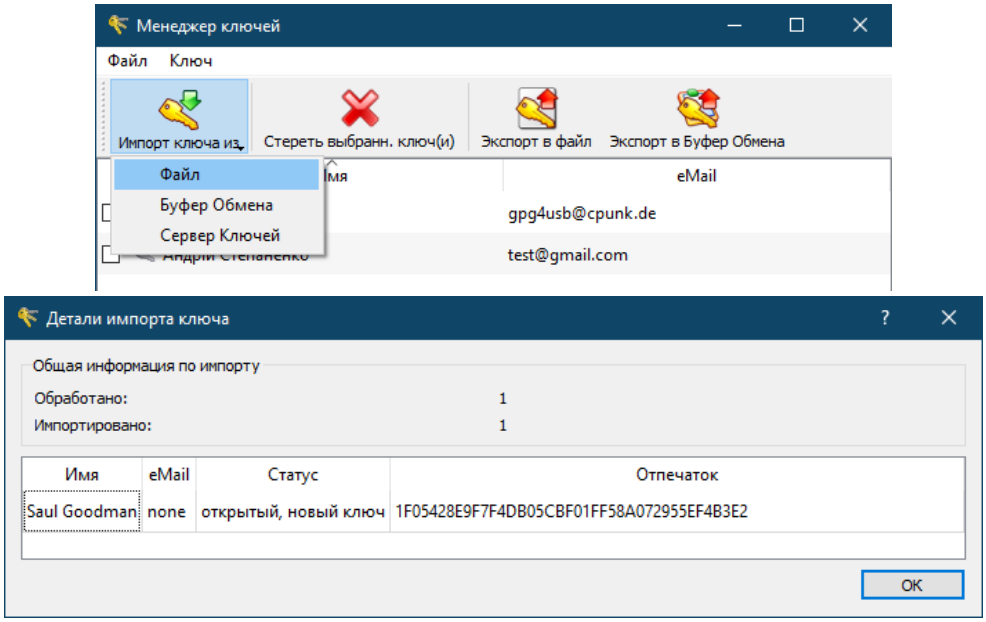
Запустити «Менеджер ключів», обрати обліковий запис своїх ключів, вибрати «Експорт обраних ключів у файл» та зберегти свій публічний ключ (наприклад, Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) на флеш-накопичувач (зобр. 3).



Зобр. 3. Експорт публічного ключа

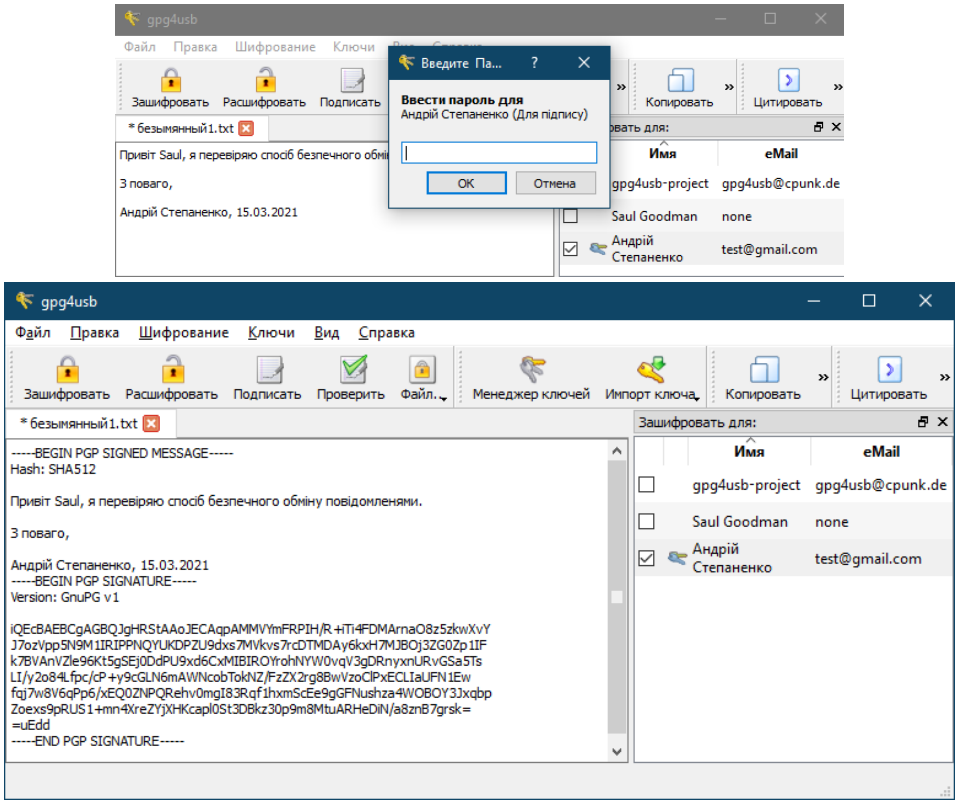
Слухачам обмінятися між собою своїми публічними ключами (Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) – це можна зробити пересиланням поштою або локальним копіюванням на свої носії.

У менеджері ключів здійснити імпорт у програму файлів публічних ключів, отриманих від інших слухачів (зобр. 4).



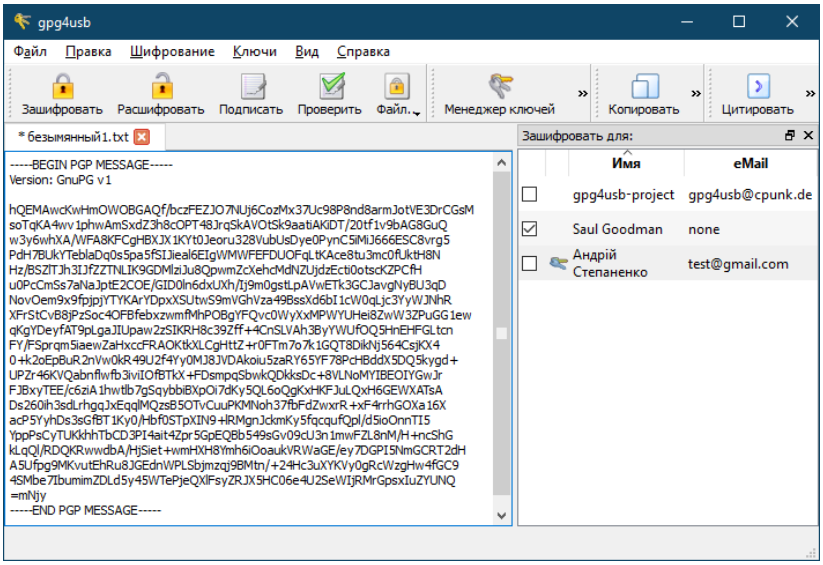
Зобр. 4. Імпорт публічних ключів співрозмовників

Створити довільне повідомлення для співрозмовника, вказати дату, час та зазначити свій ключ у правому віконці програми. Обрати «Підписати» повідомлення, ввести пароль для свого приватного ключа та отримати підпис (зобр. 5).



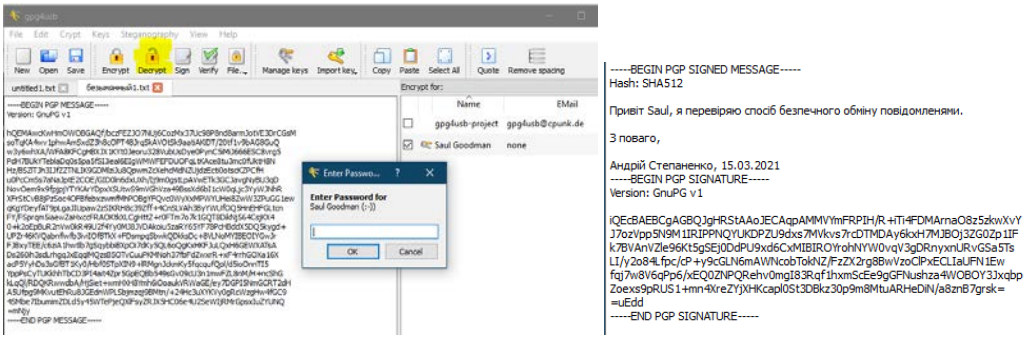
Зобр. 5. Підпис повідомлення

Зняти позначку зі свого ключа та поставити на ключі співрозмовника у правому віконці програми, обрати «Зашифрувати» (зобр. 6). Отримане зашифроване повідомлення відіслати своєму співрозмовнику.



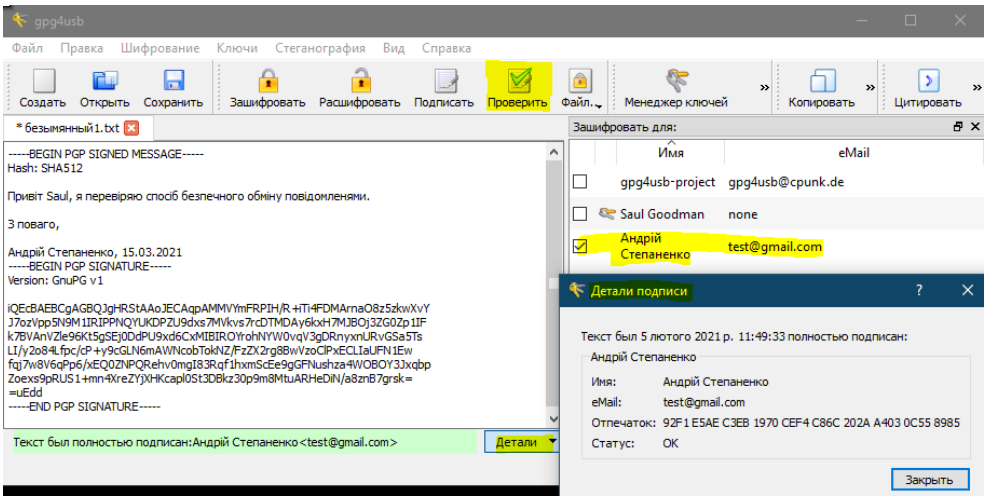
Зобр. 6. Шифрування повідомлення

Співрозмовник, отримавши зашифроване повідомлення або копіює його зміст у буфер пам'яті та вставляє у порожнє поле текстового файлу gpg4usb, або відкриває його як текстовий файл в gpg4usb. Після чого у правому полі програми позначає рядок із зазначенням своїх ключів, обирає «Розшифрувати», вводить пароль до свого приватного ключа та отримує розшифроване повідомлення (зобр. 7).

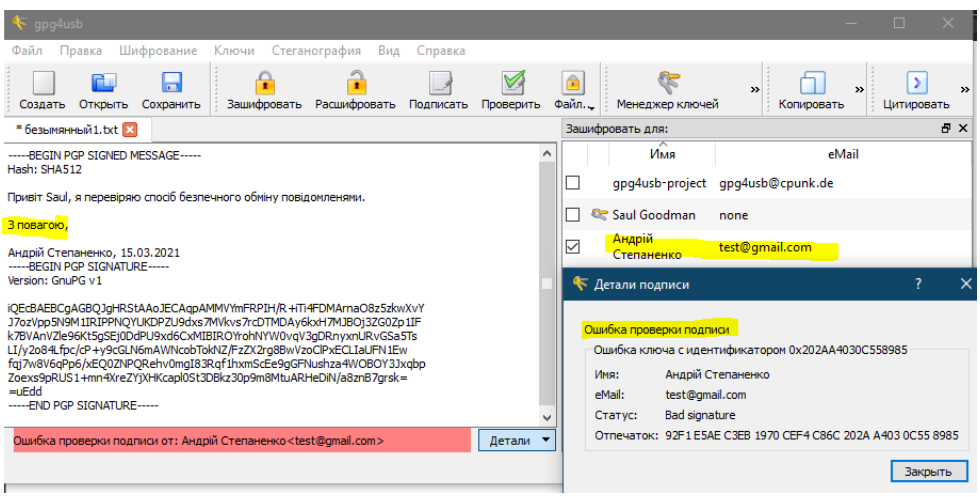


Зобр. 7. Розшифрування повідомлення

У правому полі програми співрозмовник позначає рядок із зазначенням ключа відправника, обирає «Перевірити» та «Деталі» підпису (зобр. 8). Виправити або додати у повідомленні одну літеру та повторити перевірку підпису у зміненому повідомлені (зобр. 9).



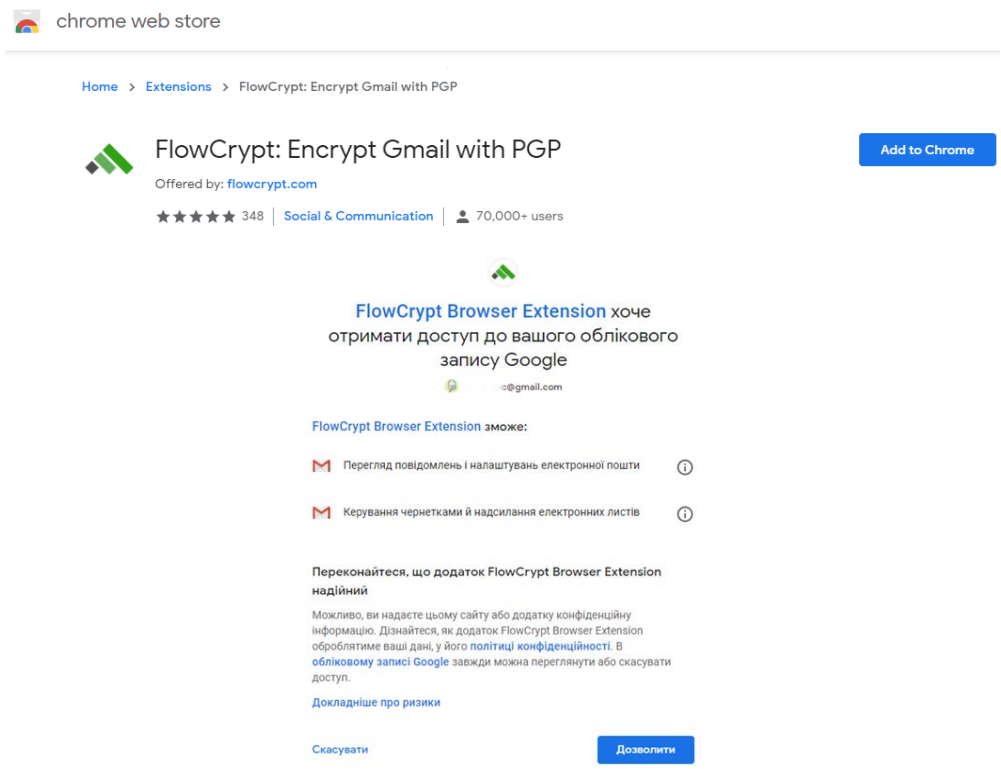
Зобр. 8. Успішна перевірка підпису відправника повідомлення



Зобр. 9. Невдала перевірка підпису відправника повідомлення

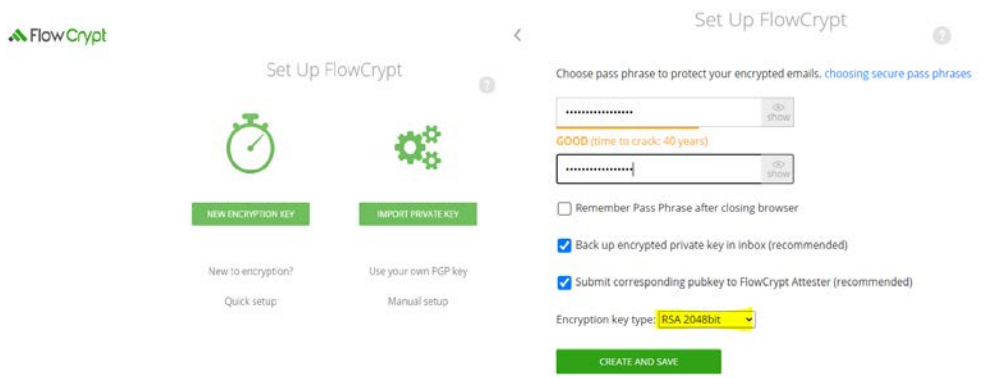
Установити і налаштувати в обліковому записі Google розширення електронного підпису та шифрування. В обліковому записі ProtonMail здійснити налаштування інтегрованого сервісу електронного підпису та шифрування листів, які спрямовуються на зовнішні поштові домени. Після налаштувань переслати підписані та зашифровані листи між поштовими доменами protonmail.com та gmail.com. Переконатися у забезпеченні конфіденційності та цілісності такого листування.

Додати в Google Chrome розширення FlowCrypt: Encrypt Gmail with PGP (https://chrome.google.com/webstore/detail/flowcrypt-encrypt-gmail-w/bnjglocicdkmhmoohhfkfkbbkejdhdgc?hl=ua), клацнути на розширення та надати дозвіл FlowCrypt отримувати доступ до облікового запису Google (зобр. 10).



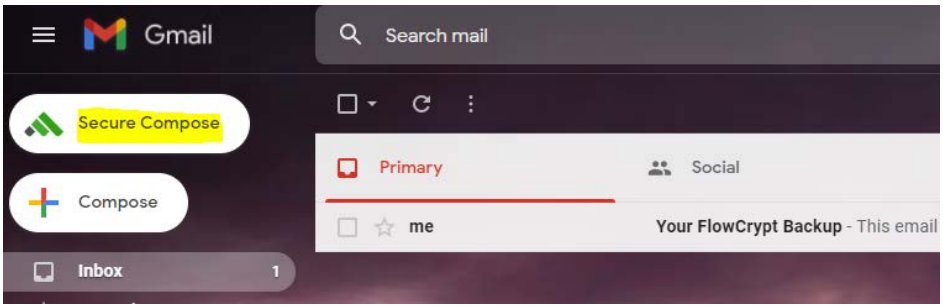
Зобр. 10. Встановлення та надання дозволу FlowCrypt

У FlowCrypt згенерувати і зберегти ключі: обрати New encryption key, Encryption key type – RSA 2048bit – Create and save (зобр. 11).



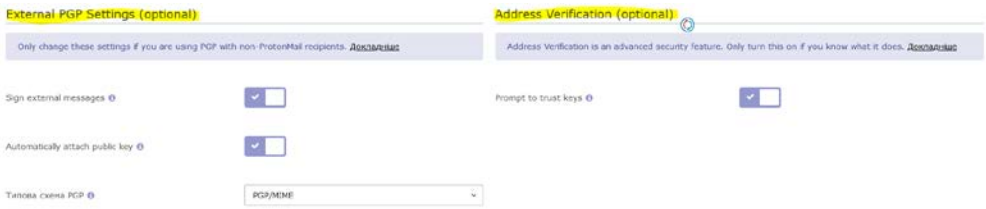
Зобр. 11. Створення і збереження ключів для облікового запису

Після налаштувань розширення в поштовому клієнті з'явиться кнопка Secure Compose (зобр. 12).



Зобр. 12. Кнопка FlowCrypt Secure Compose

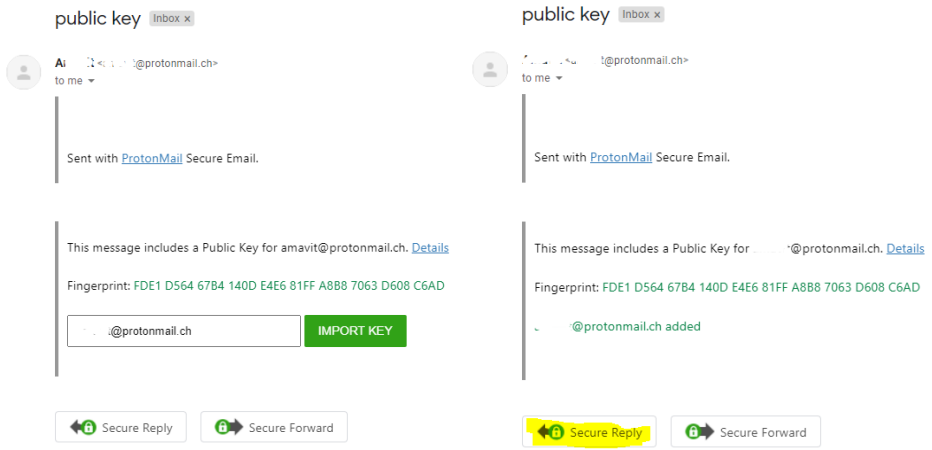
Авторизуватися у своєму обліковому записі ProtonMail. Перейти у «Налаштування» – «Безпека» і ввімкнути «External PGP Settings (optional)», Address Verification (optional) (зобр. 22).



Зобр. 13. Включення опцій підпису та шифрування

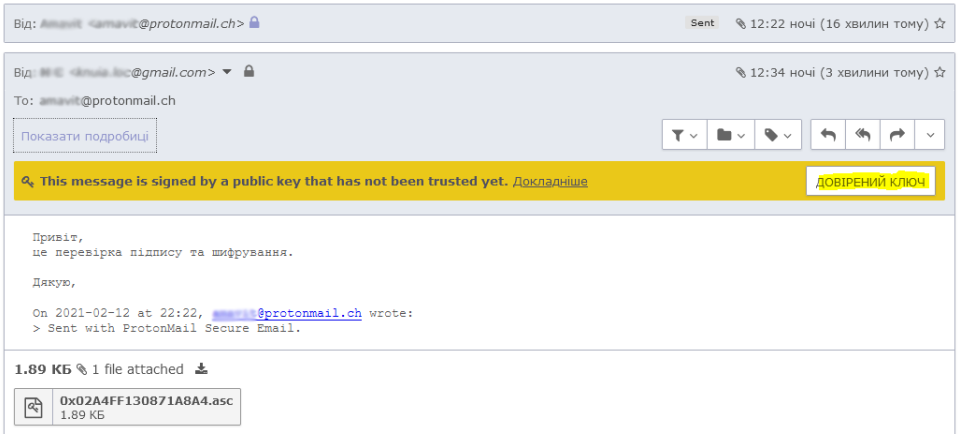
Відправити на адресу @gmail.com лист, до якого буде автоматично додано публічний ключ облікового запису @protonmail.com.

У @gmail.com після відкриття листа від @protonmail.com здійснити імпорт відкритого ключа @protonmail.com, та відповісти з підписом і шифруванням, натиснувши Secure Reply (зобр. 13).



Зобр. 14. Отримання публічного ключа та відповідь з підписом та шифруванням

У @protonmail.com буде автоматично розшифровано листа і перевірено підпис, але зазначено, що перевірка підпису була зроблена публічним ключем, який ще не є довіреним. Натиснути «ДОВІРЕНИЙ КЛЮЧ» (зобр. 15).



Зобр. 15. Розшифрований і перевірений на правдивість підпису лист з пропозицією позначити публічний ключ як довірений

Далі всі листи між обліковими записами @gmail.com і @protonmail.com будуть автоматично підписуватися і шифруватися перед відправкою, а під час отримання перевірятись та розшифровуватись.

МОДУЛЬ № 4:

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

ПРАКТИЧНА ВПРАВА

«ВБУДОВАНА В ОС WINDOWS 10 СИСТЕМА ЗАХИСТУ ВІД ВІРУСІВ І ЗАГРОЗ»

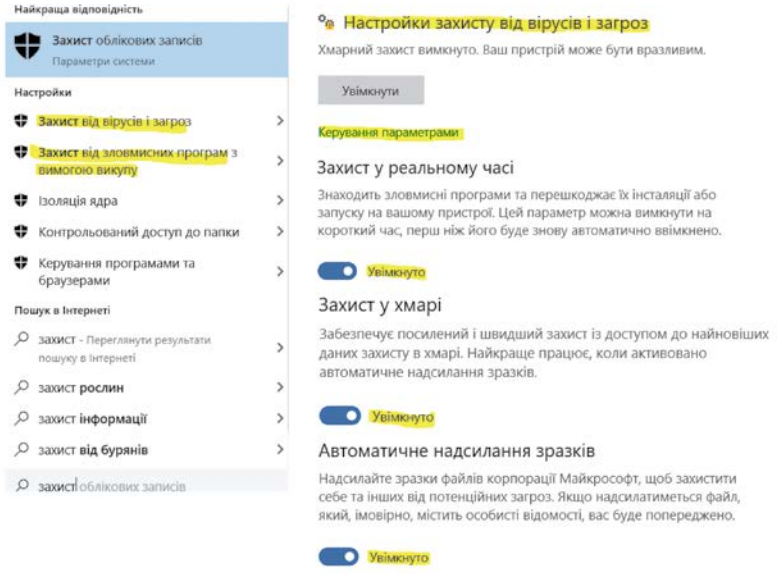
Навчальна мета заняття: налаштувати і перевірити ефективність вбудованої в ОС Windows 10 системи захисту від вірусів і загроз.

Час проведення: 1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», тестові файли.

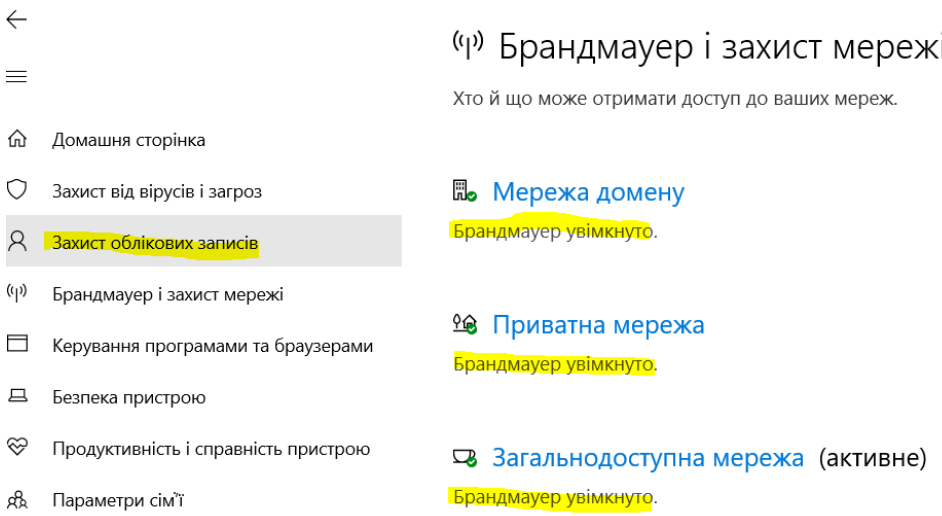
Порядок проведення заняття

На панелі задач у полі пошуку ввести запит «захист», обрати «Захист від вірусів і загроз» – «Налаштування захисту від вірусів і загроз» – «Керування параметрами», увімкнути (або переконатися, що ввімкнено) «Захист у реальному часі», «Захист у хмарі», «Автоматичне надсилання зразків» (зобр. 1).



Зобр. 1. Налаштування захисту від вірусів

Перейти із розділу «Налаштування захисту від вірусів і загроз» до розділу «Брандмауер і захист мережі» і переконатися, що брандмауер увімкнений (зобр. 2). Якщо брандмауер вимкнений, то клацнути на відповідні посилання («Мережа домену», «Приватна мережа», «Загальнодоступна мережа») та ввімкнути брандмауер.



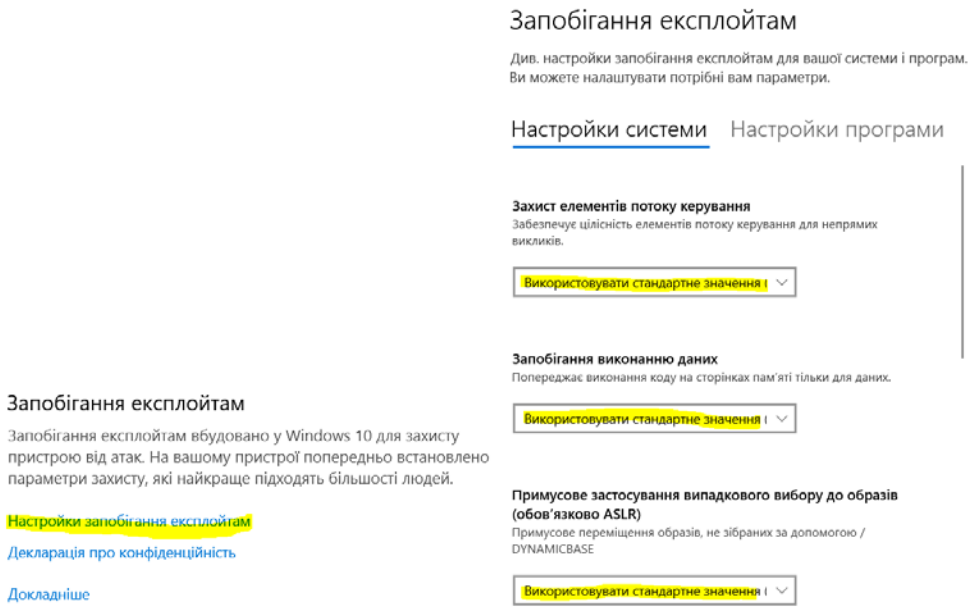
Зобр. 2. Налаштування захисту мережі

Перейти із розділу «Налаштування захисту від вірусів і загроз» до розділу «Керування програмами та браузерами», де обрати (зобр. 3):

- «Блокувати» («Попереджати») для параметру «Перевірити програми та файли»;
- «Блокувати» («Попереджати») для параметру «SmartScreen для Microsoft EDGE»;
- «Попереджати» для параметру «Фільтр SmartScreen для програм з Microsoft Store».

Зобр. 3. Налаштування SmartScreen

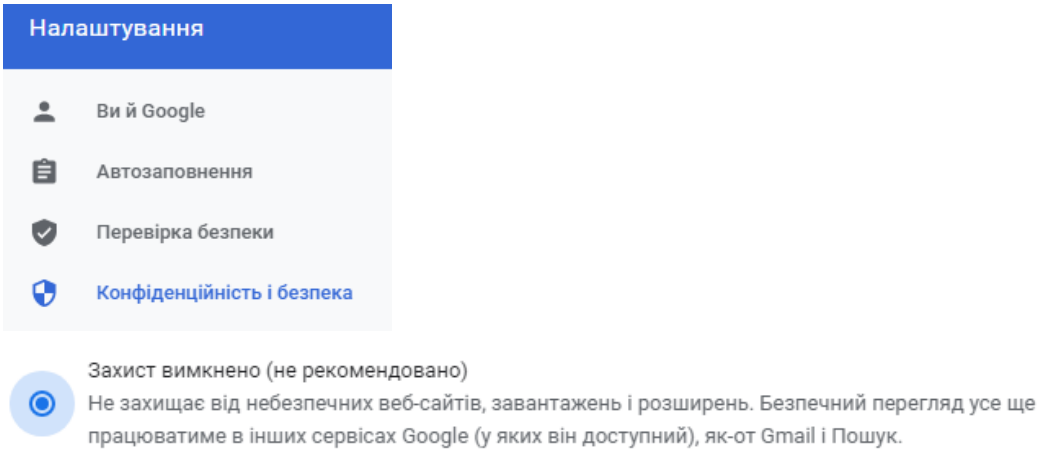
У розділі «Керування програмами та браузерами» перейти до «Налаштування запобігання експлойтам» та переконатися, що для усіх налаштувань встановлено «Використовувати стандартне значення (Увімкнуто)» (зобр. 4).



Зобр. 4. Налаштування «Настройки запобігання експлойтам»

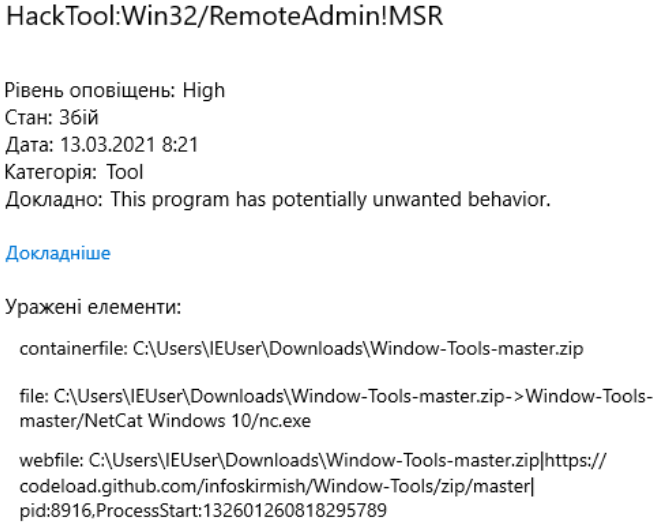
Після здійснення усіх дій вийти із меню налаштувань системи.

У налаштуваннях веббраузеру Google Chrome «Конфіденційність і безпека» – «Безпечний перегляд» обрати «Захист вимкнено (не рекомендовано)» (зобр. 5) та спробувати завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B.



Зобр. 5. Вимкнення захисту у веббраузері Google Chrome

Після завантаження файлу зі шкідливим кодом переконатися, що системою захисту від вірусів було виявлено та заблоковано цей шкідливий файл (зобр. 6).



Зобр. 6. Виявлення та блокування шкідливого файлу

ПРАКТИЧНА ВПРАВА
«АНТИВІРУС "ZILLYA!"»

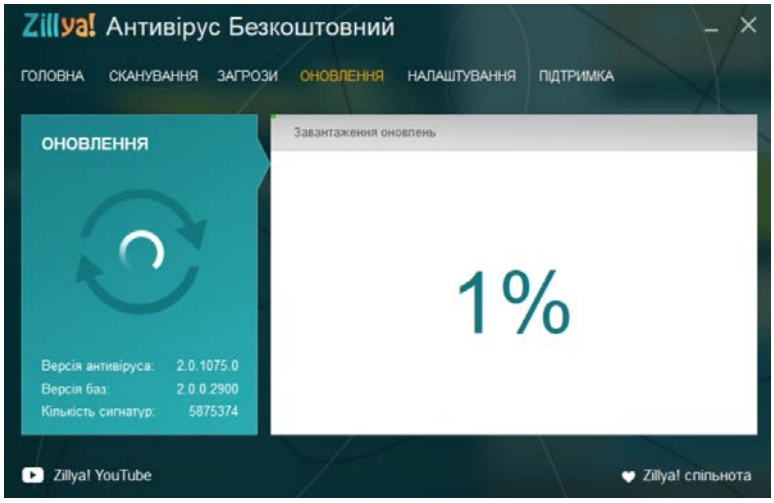
Навчальна мета заняття: встановити і перевірити ефективність сертифікованого для використання державними органами антивірусу «Zillya!».

Час проведення: 1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», тестові файли.

Порядок проведення заняття

Завантажити і виконати встановлення безкоштовної версії антивірусу «Zillya!» (https://zillya.ua/antivirus-free). Відкрити антивірус, в меню «Оновлення» запустити процес оновлення баз сигнатур вірусів (зобр. 1).



Зобр. 1. Оновлення баз сигнатур вірусів

Спробувати завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B. Встановити факт виявлення, чи не виявлення шкідливого файлу.

Самостійно виконати ті самі дії з антивірусом «ZoneAlarm» (https://www.zonealarm.com/software/free-firewall).

У налаштуваннях веббраузеру Google Chrome «Конфіденційність і безпека» - «Безпечний перегляд» обрати «Покращений захист».

МОДУЛЬ № 5:

БЕЗПЕКА КОРИСТУВАННЯ СОЦІАЛЬНИМИ МЕРЕЖАМИ

ПРАКТИЧНА ВПРАВА

«ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ОБЛІКОВОГО ЗАПИСУ FACEBOOK»

Навчальна мета заняття: налаштувати для облікового запису Facebook двофакторну автентифікацію через Google Authenticator.

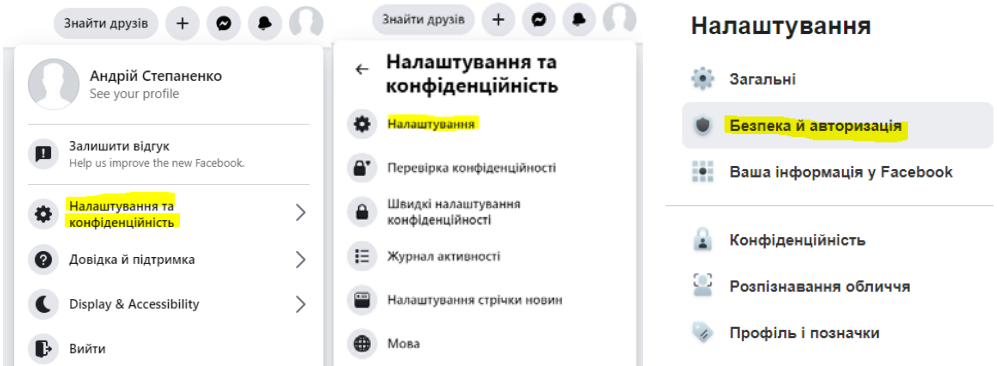
Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

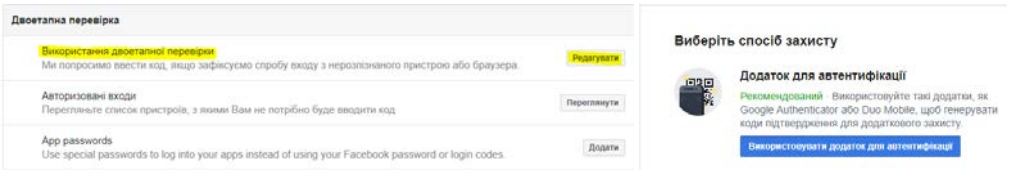
Порядок проведення заняття

Створити, якщо немає, обліковий запис у соціальній мережі «Facebook». Встановити для Facebook-облікового запису двофакторну автентифікацію через Google Authenticator.

В обліковому записі перейти в «Налаштування та конфіденційність» – «Налаштування» – «Безпека й авторизація» (зобр. 1) – «Двоетапна перевірка» – «Використання двоетапної перевірки» – «Редагувати» – «Використовувати додаток для автентифікації» (зобр. 2).

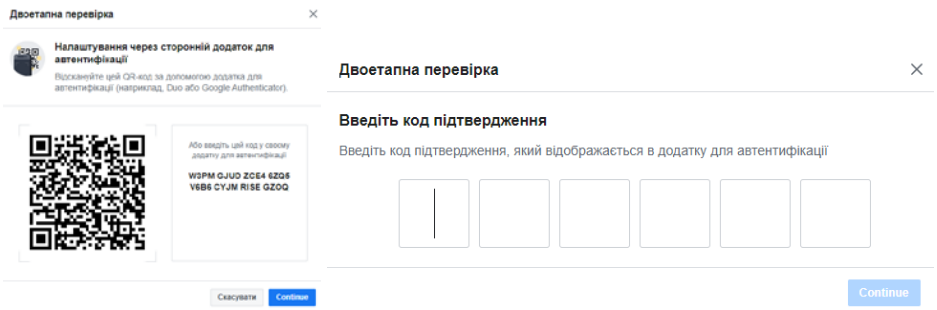


Зобр. 1. Шлях до налаштувань «Безпека й авторизація»



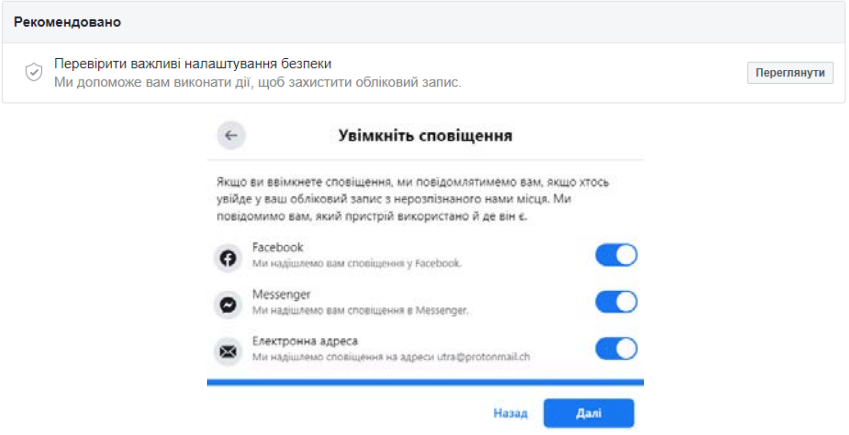
Зобр. 2. Шлях до налаштування додатка автентифікації

Переконатися, що у власному смартфоні встановлений Google Authenticator (встановлюється з Google Play або App Store), увійти до «Використовувати додаток для автентифікації», зчитати додатком смартфону Google Authenticator QR-код та ввести код підтвердження (зобр. 3).



Зобр. 3. Налаштування двоетапної перевірки

Після налаштування двоетапної перевірки повернутися у розділ «Безпека й авторизація» та переглянути важливі налаштування безпеки облікового запису, де увімкнути сповіщення про вхід у ваш обліковий запис з нерозпізнаного місця (зобр. 4).



Зобр. 4. Увімкнення сповіщення про вхід в обліковий запис з нерозпізнаного місця

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації.

ПРАКТИЧНА ВПРАВА

«ВИДАЛЕННЯ МЕТАДАНИХ ФОТОЗОБРАЖЕНЬ»

Навчальна мета заняття: навчитися перевіряти наявність метаданих у файлах фотозображень та видаляти їх.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

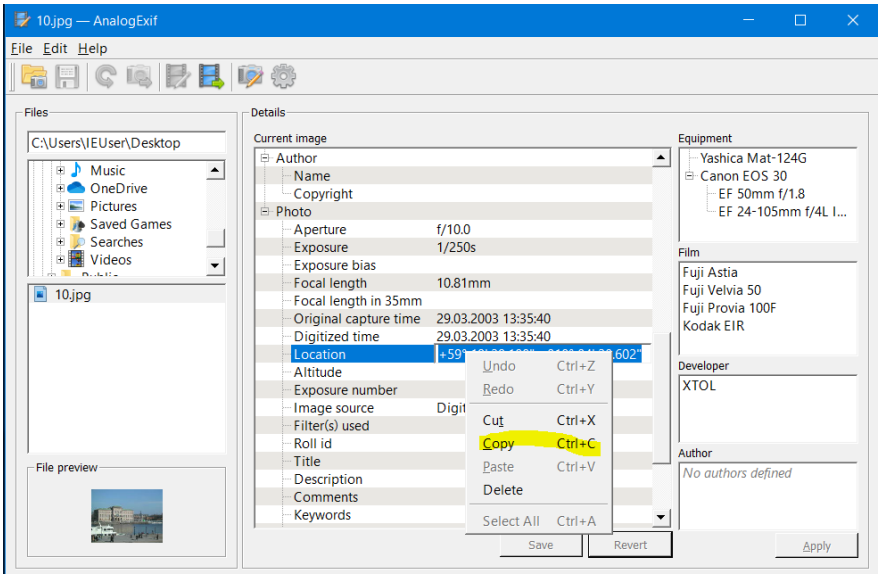
Порядок проведення заняття

В особистому смартфоні включити GPS, підійти до вікна у приміщенні й дочекатися встановлення координат свого місцезнаходження, перевіривши цей факт запуском додатку «Карти», де відобразиться точне місцезнаходження смартфона.

Зробити декілька фотознімків фотокамерою смартфона, підключити смартфон до комп'ютера та завантажити фотозображення на комп'ютер. Або скопіювати на комп'ютер підготовлені файли фотозображень з метаданими.

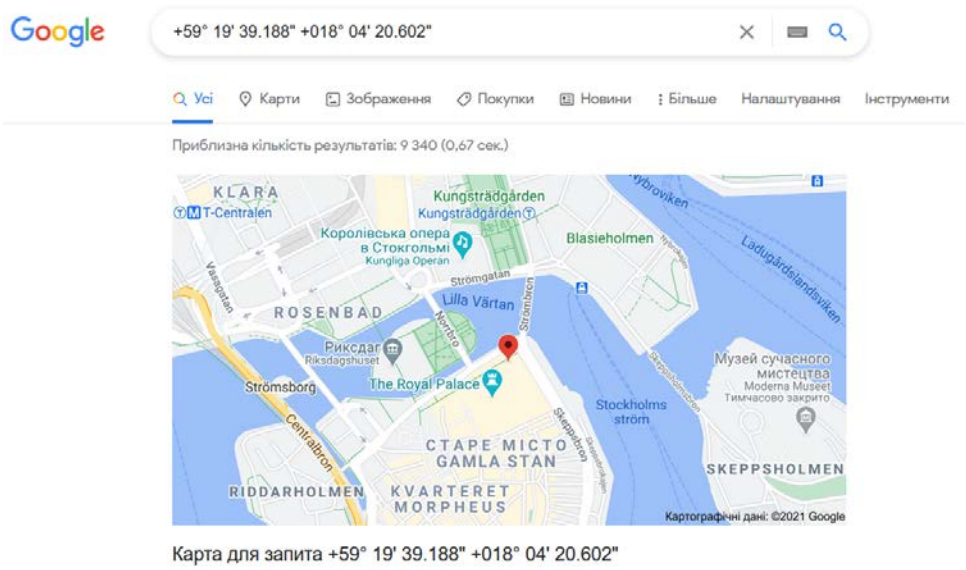
Перевірити наявність метаданих у файлах фотозображень та видалити їх.

Завантажити, встановити і запустити утиліту перегляду та редагування метаданих «AnalogExif» (https://sourceforge.net/projects/analogexif). Відкрити у AnalogExif фотозображення, переглянути метадані, двічі клацнути на поле Location та скопіювати у буфер координати (зобр. 1).



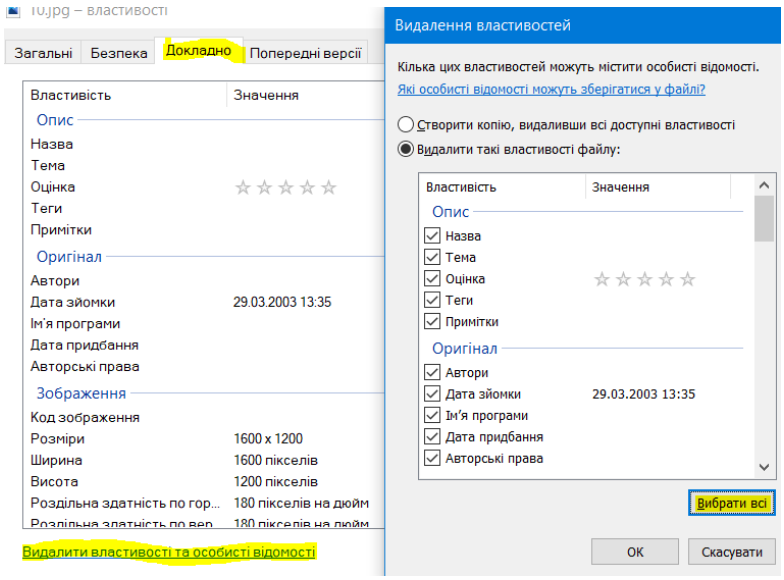
Зобр. 1. Перегляд метаданих фотозображення

Відкрити веббраузер «Google Chrome», вставити координати в адресний рядок і здійснити пошук місця фотозйомки (зобр. 2).



Зобр. 2. Пошук місця фотозйомки за координатами з метаданих фотозображення

У Провіднику файлів через контекстне меню (клацнути правою кнопкою миші) подивитися «Властивості файлу фотозображення», перейти у вкладку «Докладно» та клацнути на «Видалити властивості та особисті відомості» – «Вибрати всі» – «ОК» (зобр. 7).



Зобр. 3. Видалення метаданих фотозображень

Знову відкрити у AnalogExif фотозображення та переконатися, що метадані відсутні та можна їх безпечно завантажувати у соціальні мережі.

ПРАКТИЧНА ВПРАВА
«ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ОБЛІКОВОГО ЗАПИСУ INSTAGRAM ТА TWITTER»

Навчальна мета заняття: налаштувати для облікового запису Instagram та Twitter двофакторну автентифікацію.

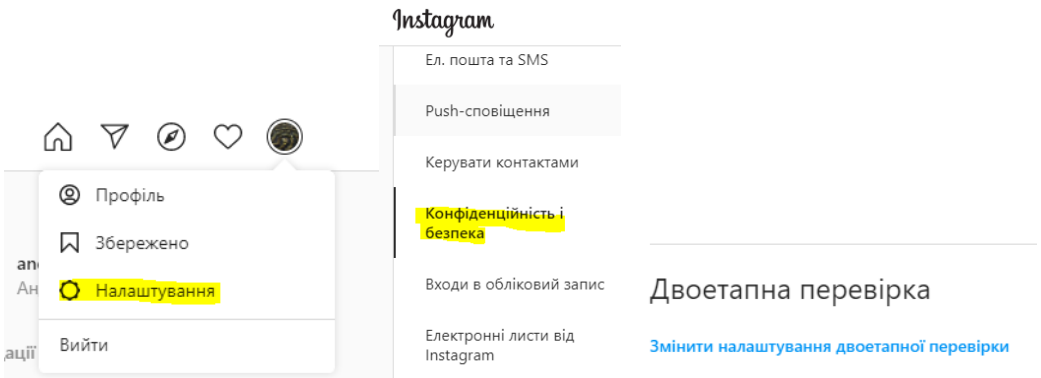
Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

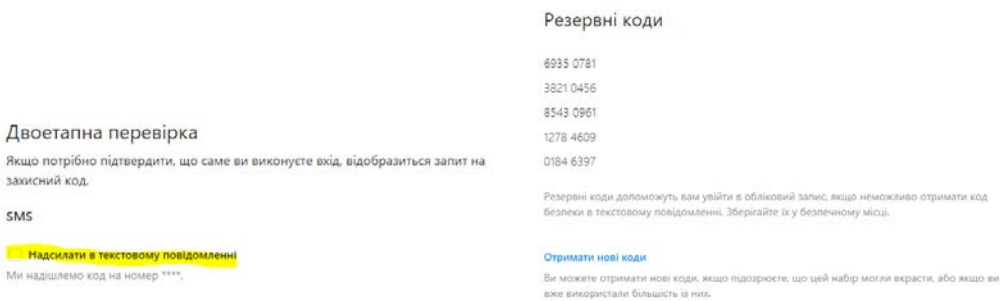
Порядок проведення заняття

Із використанням раніше створеного Facebook-облікового запису створити Instagram-обліковий запис та встановити двофакторну автентифікацію облікового запису.

Перейти «Налаштування» – «Конфіденційність і безпека» – «Змінити налаштування двоетапної перевірки» (зобр. 1). Увімкнути двоетапну перевірку «Надсилати в текстовому повідомленні» та зберегти у парольному менеджері резервні коди доступу, які можна використати за неможливості отримання текстових повідомлень.



Зобр. 1. Вхід до налаштувань двоетапної перевірки



Зобр. 2. Налаштування двоетапної перевірки

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації.

Створити обліковий запис у Twitter та, з огляду на попередньо виконані задачі, увімкнути і налаштувати двоетапну перевірку автентифікації. Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації.

МОДУЛЬ № 6:

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ

ПРАКТИЧНА ВПРАВА

«НАЛАШТУВАННЯ ЗАХИСНИХ МЕХАНІЗМІВ У МОБІЛЬНОМУ ПРИСТРОЇ»

Навчальна мета заняття: відповідно до конкретних умов навчитися налаштовувати параметри мобільного пристрою та встановлених на ньому програм для безпечного використання.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», програма виведення зображення з мобільного пристрою на екран монітора персонального комп'ютера.

Завдання, які потрібно виконати, **підкреслено**.

Вхідні дані

Потрібні програми:

Telegram

Viber

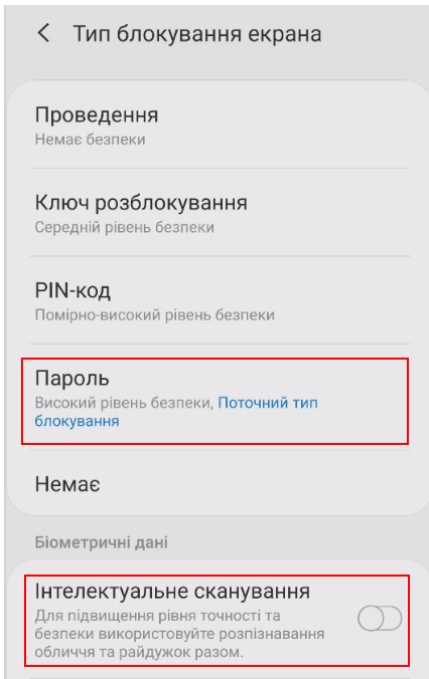
WhatsApp

Налаштування безпеки мобільного пристрою слід організовувати за двома головними напрямами:

1) налаштування операційної системи мобільного пристрою;

2) налаштування прикладних програм.

Що стосується першого напряму, то, передусім, для безпечного користування смартфоном слід встановити надійний механізм його розблокування. Для цього потрібно зайти у налаштування системи та встановити пароль, який буде достатньо довгим та складатиметься з літер, цифр та спеціальних символів (зобр. 1).

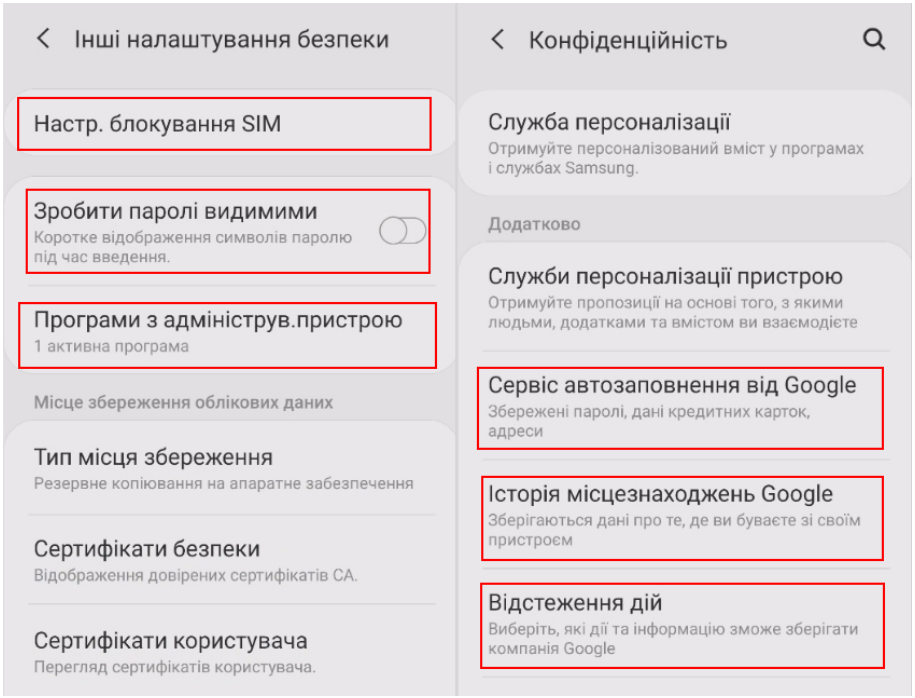


Зобр. 1. Налаштування паролю для розблокування пристрою

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Touch ID і код-пароль» → «Запит паролю: одразу» → «Змінити пароль» → «Довільний код (літери + цифри).

У випадку, якщо дозволяють функції пристрою, можна також налаштувати біометричну ідентифікацію.

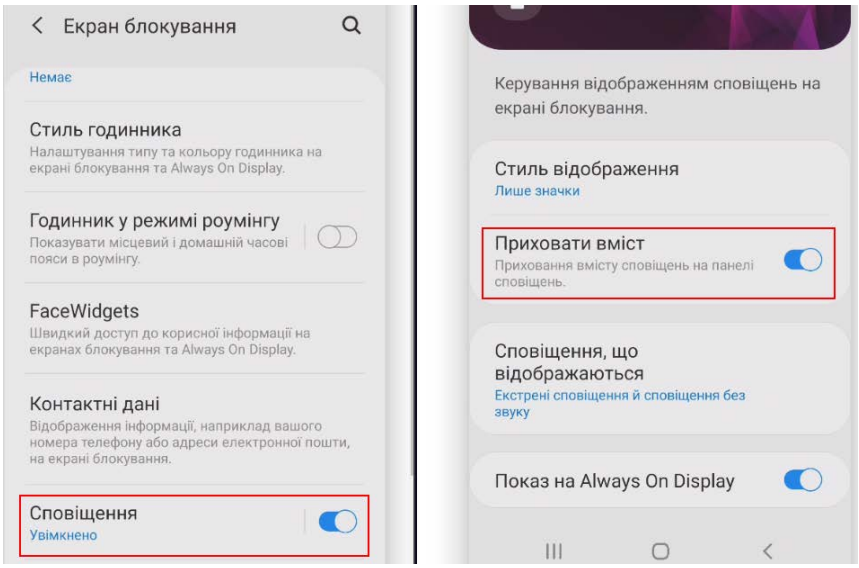
Крім наведеного, слід переглянути інші налаштування безпеки та встановити їх таким чином, щоб вони відповідали потрібному рівню захисту (зобр. 2).



Зобр. 2. Налаштування параметрів безпеки та конфіденційності

Після проведення загальних налаштувань операційної системи слід убезпечити себе від витоку інформації із заблокованого пристрою. Для цього, перш за все, потрібно вимкнути повідомлення на заблокованому екрані (зобр. 3). Також відповідні налаштування можуть бути встановлені окремо для кожного застосунку («Налаштування» → «Програми»). Виконання описаних дій дозволить стороннім особам бачити приватні повідомлення.

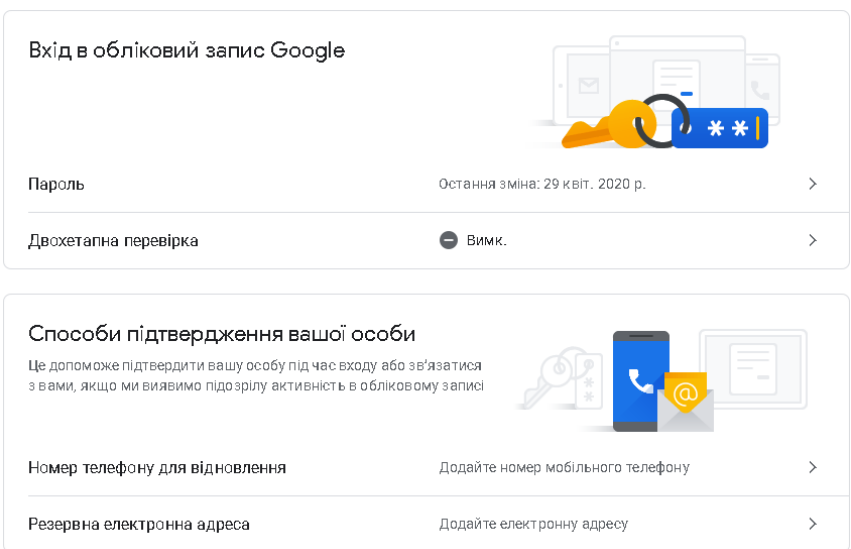
Для виконання розглянутого завдання на iPhone: «Налаштування» → «Пароль» → «Доступ з блокуванням екрану»; «Налаштування» → «Сповіщення» → «Показ мініатюр» → «Без блокування».



Зобр. 3. Вимкнення повідомлень

Слід пам'ятати, що окремі налаштування стосуються не тільки самого мобільного пристрою, але й облікового запису. Враховуючи це потрібно переглянути налаштування безпеки облікового запису та встановити відповідні параметри.

Одним з прикладів такого налаштування є встановлення двофакторної автентифікації (зобр. 4).

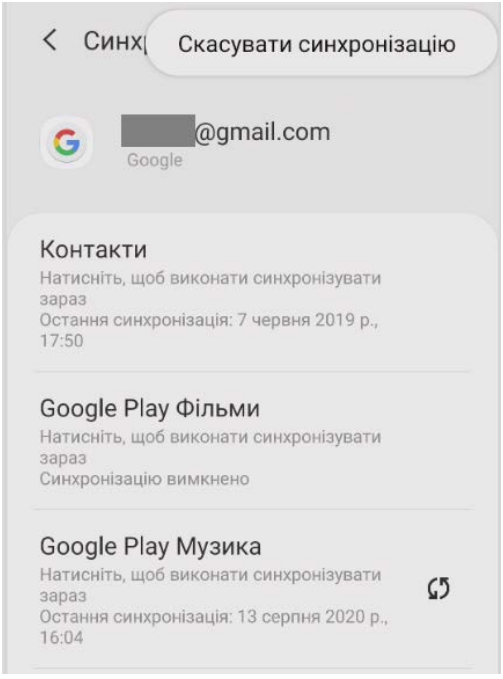


Зобр. 3. Налаштування безпеки облікового запису

Для виконання розглянутого завдання на iPhone: «Сайт Apple ID» → «Двофакторна ідентифікація» → «Увімкнути»; «Безпека» → «Перевірені номери телефонів» → «Змінити» → «Додати номер телефону з можливістю приймання текстових повідомлень».

Для заборони відслідковування своїх дій після авторизації в обліковому записі можна встановити спеціальне розширення (https://tools.google.com/dlpage/gaoptout?hl=ru).

Залежно від конкретних умов слід правильно налаштувати синхронізацію даних. Якщо Ви не бажаєте зберігати відомості на віддаленому ресурсі, потрібно вимкнути автоматичну синхронізацію даних у налаштуваннях відповідного облікового запису в мобільному пристрої (зобр. 4).

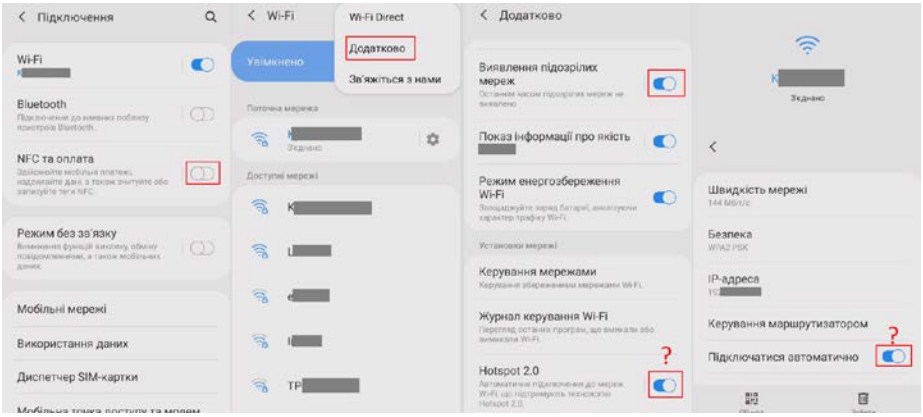


Зобр. 4. Налаштування синхронізації

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Apple ID, iCloud, медіаматеріали» → «iCloud» → «iCloud Drive» → «Фото».

Крім наведеного, слід також вимкнути автоматичне підключення до Wi-Fi мереж (зобр. 5). Якщо у Вас налаштоване автопідключення до відомих точок доступу Wi-Fi, то Ви так само автоматично можете бути під'єднаним до підробленої точки доступу.

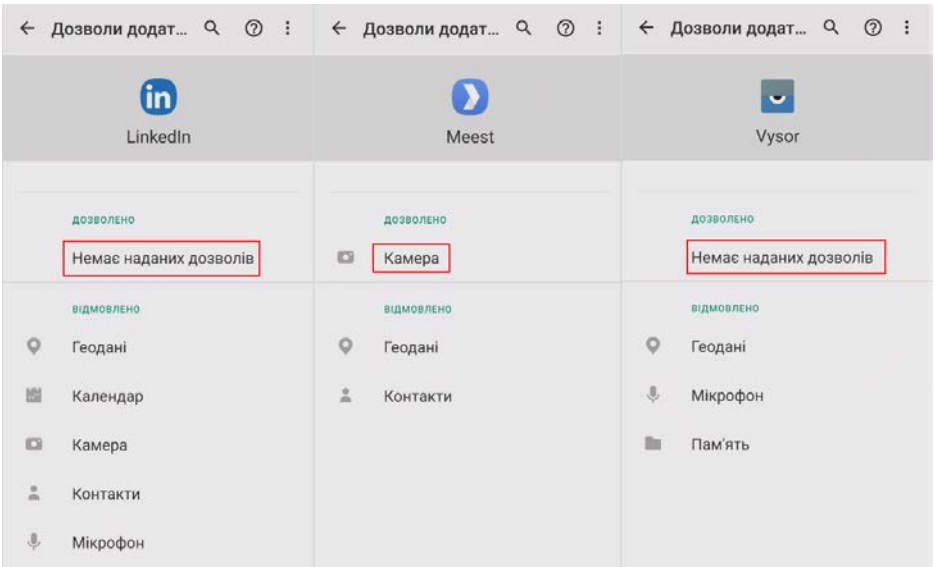
У подальшому весь трафік Інтернет може бути пропущений через обладнання зловмисника. Це дозволяє порушнику примусово перенаправляти запити з Вашого пристрою на свої ресурси. При цьому Ви можете навіть нічого не помітити.



Зобр. 5. Налаштування Wi-Fi

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Wi-Fi» → Обрати відповідну мережу → «Автопідключення» → «Вимкнути».

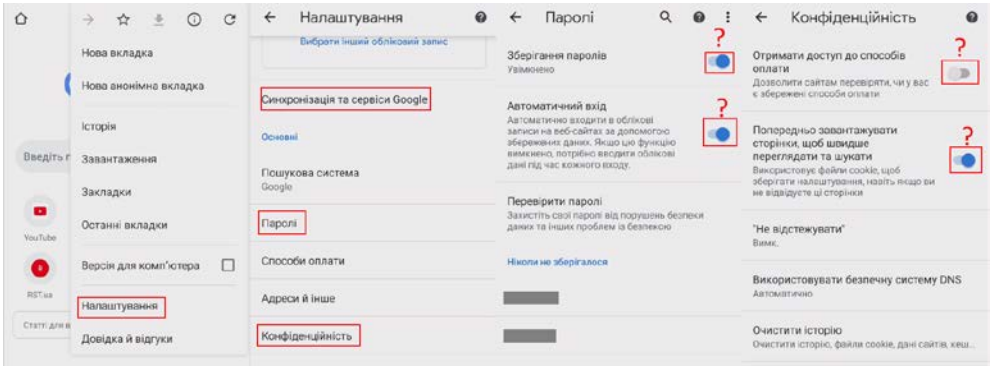
Що стосується налаштувань окремих застосунків, то тут слід передусім звернути увагу на обмеження їх доступу до чутливих даних: файлів на телефоні, контактів, геолокації тощо (зобр. 6).



Зобр. 6. Налаштування прав доступу для застосунків

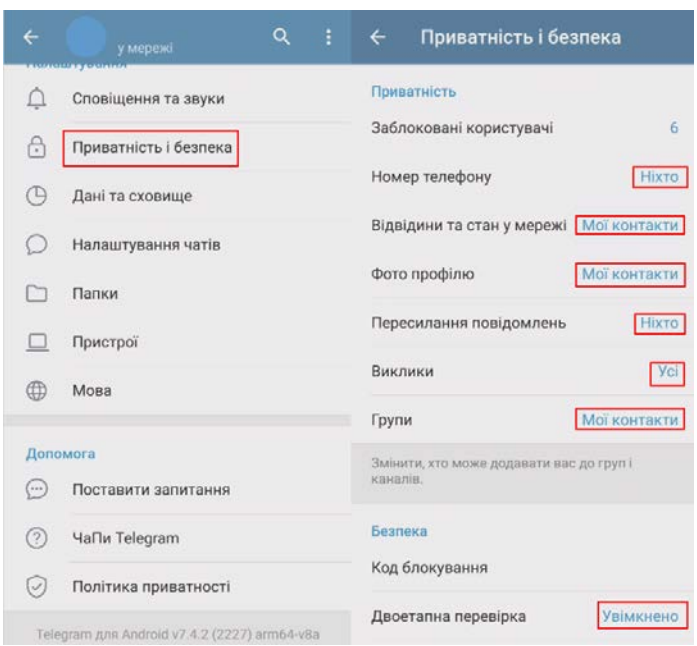
Для виконання розглянутого завдання на iPhone: «Налаштування» → «Конфіденційність» → «Геолокація», «Відслідковування» → поставити «Вимкнути» у налаштуваннях відповідних застосунків.

У використовуваних браузерах також слід налаштувати відповідну безпеку. Наприклад, у Google Chrome це можна зробити як на зобр. 7.

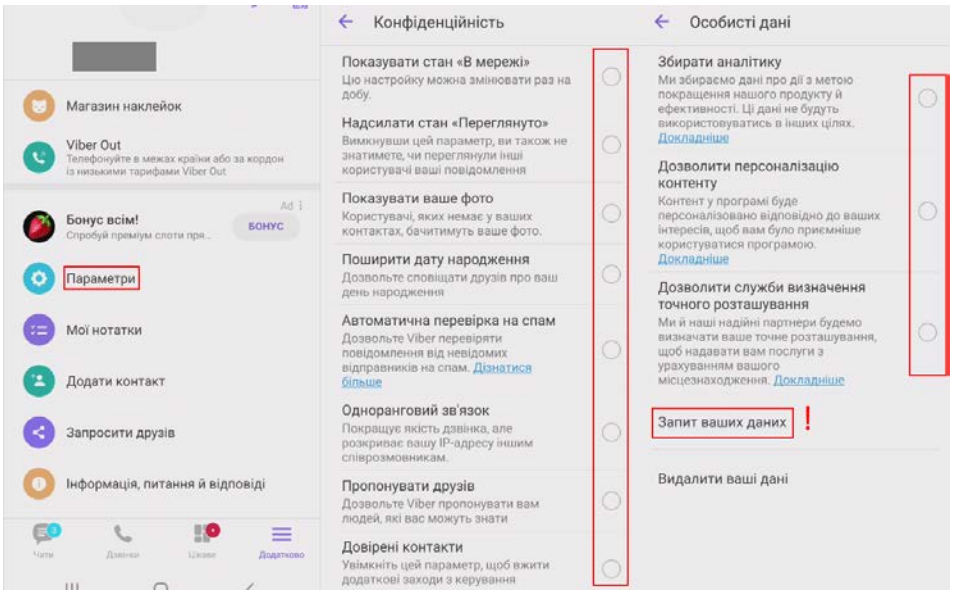


Зобр. 7. Налаштування безпеки браузера

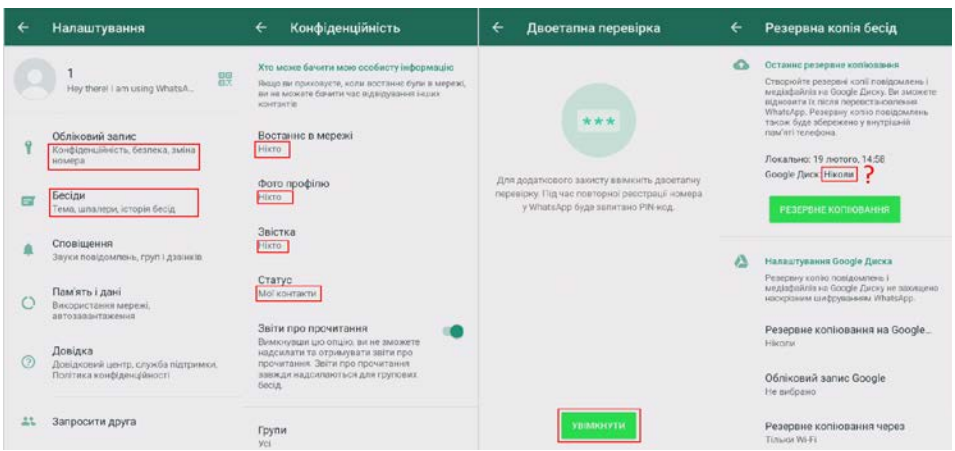
Важливою частиною захисту мобільного пристрою є правильне налаштування програм для спілкування (месенджерів). Найбільш поширеними такими рішеннями на теперішній час є Telegram (зобр. 8), Viber (зобр. 9), WhatsApp (зобр. 10).



Зобр. 8. Налаштування безпеки «Telegram»



Зобр. 9. Налаштування безпеки «Viber»



Зобр. 10. Налаштування безпеки «WhatsApp»

Щодо налаштувань резервного копіювання даних в різних застосунках, то тут рішення користувач має прийняти самостійно з урахуванням існуючих ризиків.

Завдання

1. Налаштуйте параметри безпеки для:

- операційної системи свого мобільного пристрою;
- облікових записів, прив'язаних до мобільного пристрою;
- встановлених на мобільному пристрої застосунків.

МОДУЛЬ № 7:

ФІЗИЧНА БЕЗПЕКА

ПРАКТИЧНА ВПРАВА

«СТВОРЕННЯ ЗАХИЩЕНОГО ФЛЕШ-НАКОПИЧУВАЧА»

Навчальна мета заняття: створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go та програми VeraCrypt.

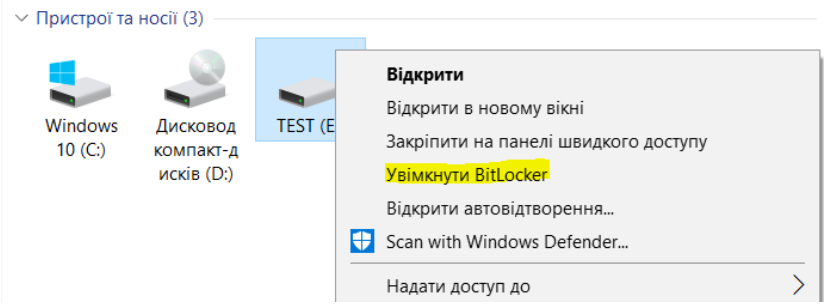
Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

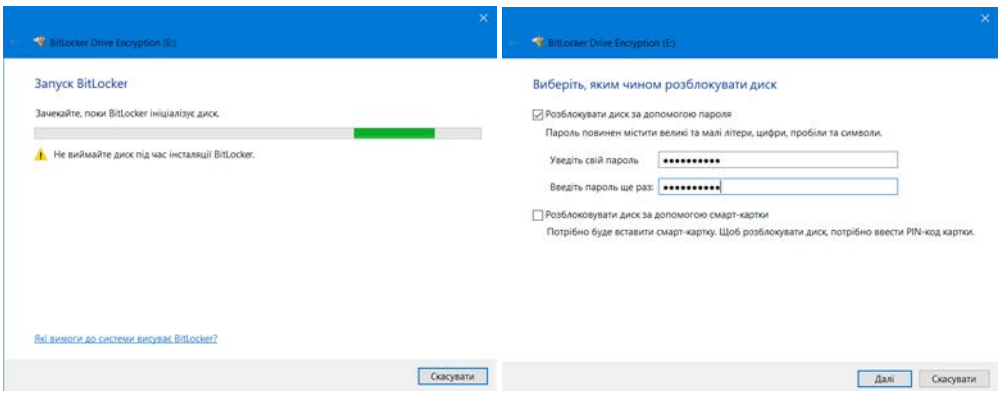
Створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go, який повністю шифрує вміст флеш-накопичувача на рівні файлової системи. У випадку фізичної втрати флеш-накопичувача дані залишаться недоступними для читання.

Вставити флеш-накопичувач у USB порт та відкрити «Провідник файлів». Увімкнути BitLocker для диску флеш-накопичувача: клацнути правою кнопкою миші диск у вікні «Провідника файлів», а потім вибрати команду «Увімкнути BitLocker». Якщо немає цього параметра у контекстному меню, то, ймовірно, у вас не Windows Pro або Enterprise, і знадобиться шукати інше рішення для шифрування (зобр. 1).



Зобр. 1. Увімкнення BitLocker

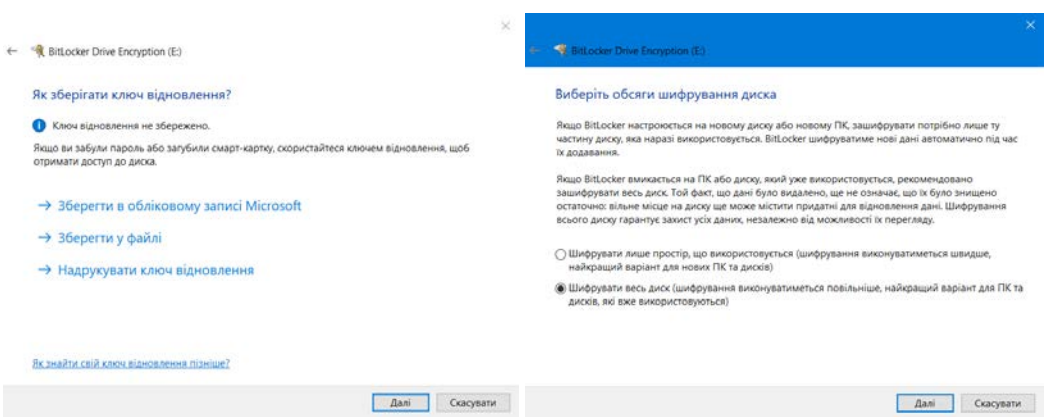
Зачекати, поки BitLocker здійснить ініціалізацію диску, далі обрати спосіб розблокування диску – за допомогою паролю, обрати надій пароль (зобр. 2).



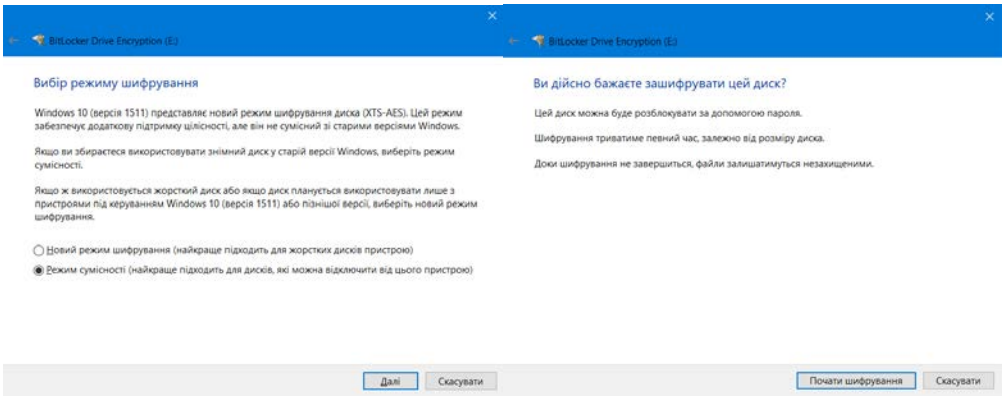
Зобр. 2. Ініціалізація BitLocker та вибір способу розблокування диску

Далі BitLocker надає можливість створити ключ відновлення, який можна використовувати для доступу до зашифрованих файлів, якщо ви, наприклад, забудете пароль (зобр. 3). Ключ відновлення можна зберегти у своєму обліковому записі Microsoft, на диску USB, файлі або навіть роздрукувати. Ці параметри є однаковими, якщо ви шифруєте системний або несистемний диск. Зберегти ключ відновлення у файл – зміст цього файлу можна скопіювати у парольний менеджер та видалити файл.

Далі обрати шифрування всього диску (зобр. 3), режим сумісності для різних версій Windows та запустити шифрування диску (зобр. 4).

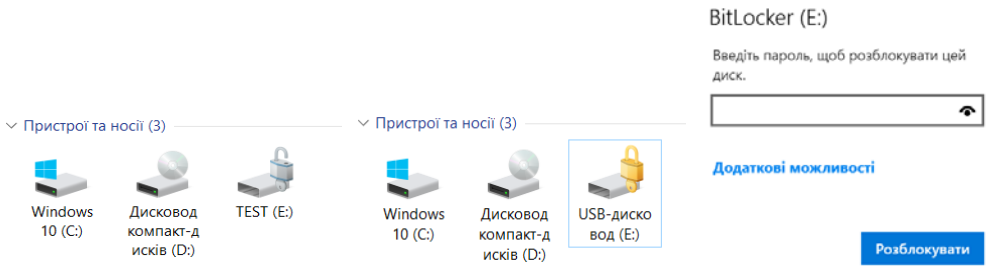


Зобр. 3. Збереження ключа відновлення та вибір обсягу шифрування диску



Зобр. 4. Вибір режиму шифрування та початок шифрування

Після завершення шифрування у «Провіднику файлів» з'явися відповідна піктограма розшифрованого диску, яка зміниться, якщо витягти диск і знову вставити, а також з'явиться запрошення ввести пароль для розшифрування диску (зобр. 5).



Зобр. 5. Піктограми розшифрованого та зашифрованого диску, запрошення ввести пароль

Записати на розшифрований диск довільні файли, витягнути флеш-накопичувач та повторити процедуру розблокування, щоб переконатися у цілісності файлів після розшифрування.

Створити захищений флеш-накопичувач за допомогою безкоштовної утиліти з відкритим кодом «VeraCrypt», яка побудована на базі останньої версії TrueCrypt.

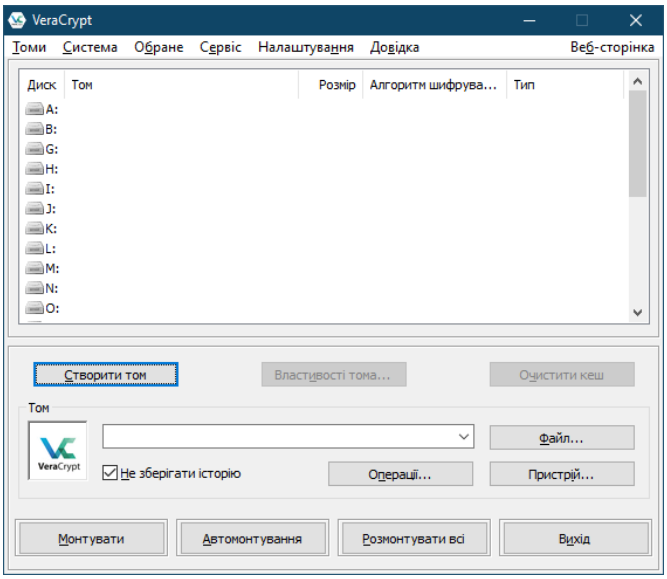
VeraCrypt використовує так званий контейнер. Стосовно VeraCrypt, контейнер – це оболонка, в якій у зашифрованому вигляді зберігаються всі файли. Фізично контейнер – це один файл. Отримати доступ до файлів, які лежать всередині контейнера-оболонки можна тільки одним способом – ввівши правильний пароль.

Процедура введення пароля і підключення контейнера називається «монтуванням».

Файли у VeraCrypt шифруються не по одному, а контейнерами. Коли програма підключає контейнер (монтує його), то контейнер виглядає як флешка – з'являється новий диск, з яким можна робити будь-які операції – копіювати туди файли, відкривати файли, видаляти файли, редагувати файли. Роблячи це, не потрібно думати про шифрування – все, що всередині контейнера, вже надійно зашифровано і зберігається / шифрується в реальному часі. І як тільки вимкнути контейнер, то вхід до нього надійно закриється.

Завантажити архів портативної версії утиліти (portable version for Windows, https://www.veracrypt.fr/en/Downloads.html) та запустити розпакування.

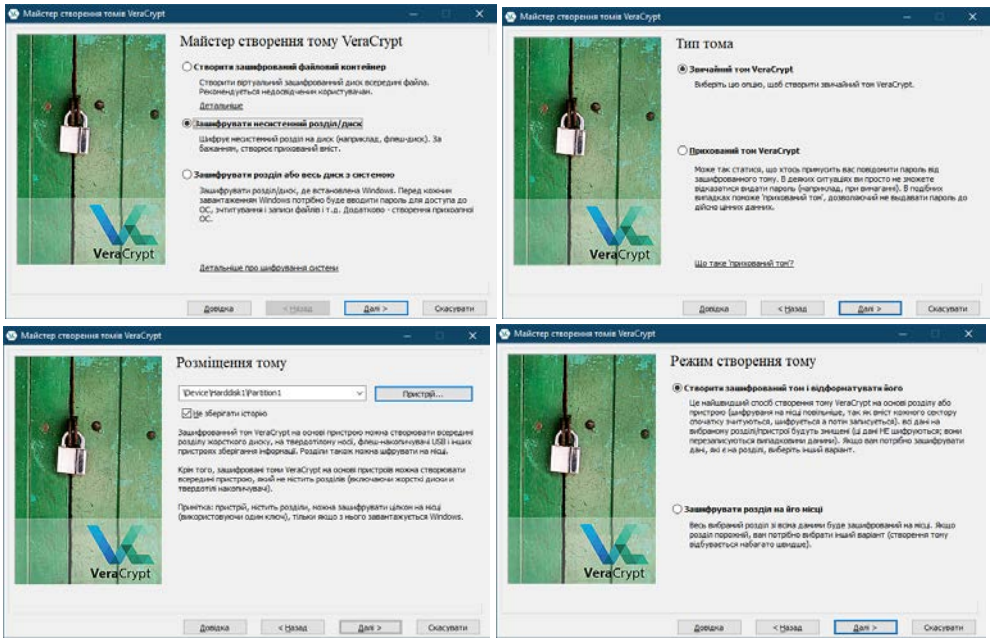
З теки VeraCrypt запустити файл VeraCrypt-x64.exe та у меню 'Settings' змінити мову програми на українську. Для цього клацнути на меню 'Settings', там вибрати 'Language ...' та обрати «Українська». Далі натиснути «Створити том» (том – це те ж саме що і контейнер) (зобр. 6).



Зобр. 6. Головне вікно VeraCrypt

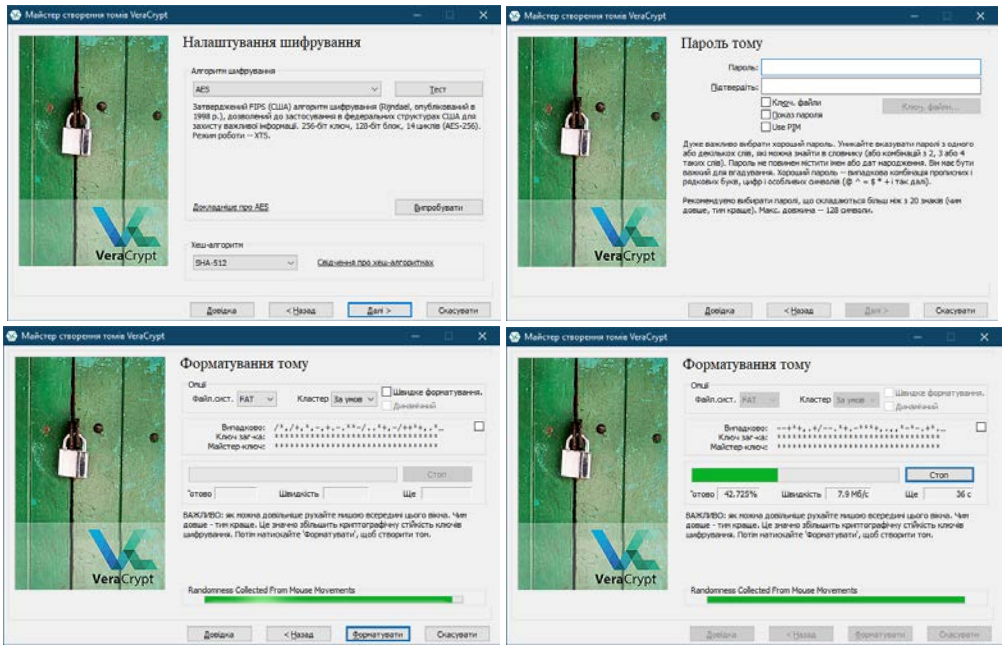
Обрати «Зашифрувати несистемний розділ/диск», «Звичайний том VeraCrypt». Вибрати розміщення тому, вказавши як пристрій флеш-накопичувач. **ВАЖЛИВО: перевірити правильність вибору пристрою, який потім буде форматуватися.**

Вибрати режим створення тому «Створити зашифрований том і відформатувати його» (зобр. 7).



Зобр. 7. Майстер створення тому

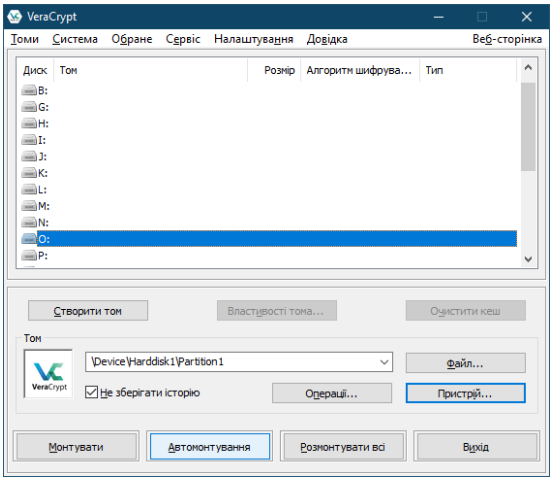
Налаштування шифрування залишити за замовчуванням. Встановити пароль тому дотримуючись рекомендацій, що будуть запропоновані у вікні вибору паролю. Важливо запам'ятати пароль і ніде не записувати. Як рекомендація – взяти перші (останні) літери улюбленої довгої фрази із заміною деяких літер цифрами і символами. Для форматування тому випадковим чином рухати мишею деякий час, а потім ініціювати форматування носія.



Зобр. 8. Налаштування шифрування та форматування тому

Після форматування ознайомитися із порядком монтування тому. Захищений флеш-накопичувач створено.

Для користуванням захищеним носієм у головному вікні VeraCrypt вибрати у розділі «Пристрій» диск флеш-накопичувача, вільну літеру для диску, що буде змонтований, та натиснути «Монтувати» або «Автомонтування» (зобр. 9).



Зобр. 9. Підключення зашифрованого диску

На запит ввести пароль і буде створений новий логічний диск, з яким можна працювати: записувати і редагувати файли, запускати програми.

По закінченні роботи із змонтованим диском у головному вікні VeraCrypt натиснути «Розмонтувати всі».

Перевірити надійність захисту інформації здійснити шляхом обміну змінними носіями і спробою відкрити диски.

ПРАКТИЧНА ВПРАВА
«БЛОКУВАННЯ ДОСТУПУ ДО ОПЕРАЦІЙНОЇ СИСТЕМИ ЗА ВІДСУТНОСТІ АКТИВНОСТІ»

Навчальна мета заняття: налаштувати блокування ОС Windows за відсутності активності.

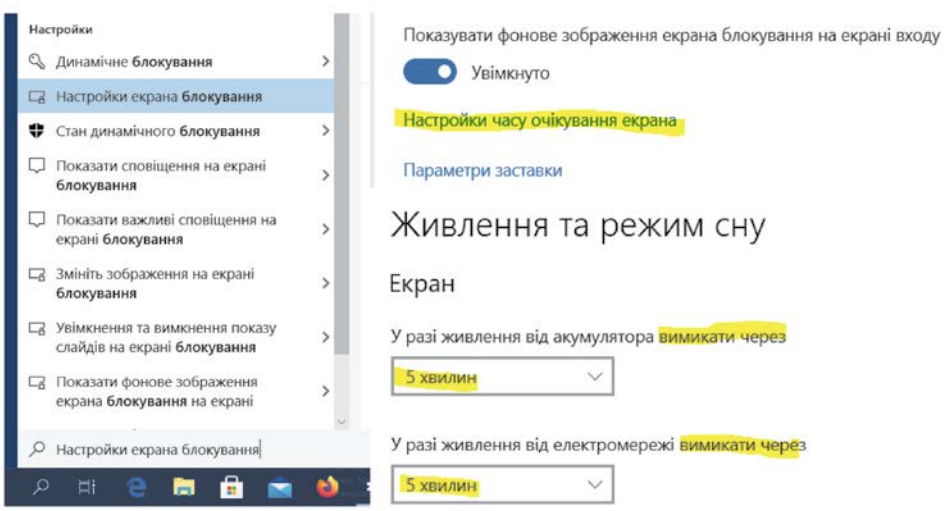
Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Налаштувати та перевірити функціонування автоматичного блокування ОС Windows після 5 хвилин відсутності активності.

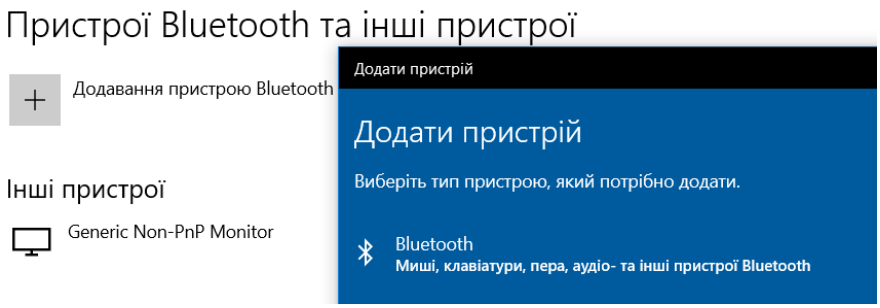
На панелі задач у полі пошуку ввести запит «блокування», вибрати «Налаштування екрана блокування» – «Налаштування часу очікування екрана» та встановити «…вимикати через 5 хвилин» (зобр. 1).



Зобр. 1. Налаштування автоматичного блокування ОС Windows після 5 хвилин відсутності активності

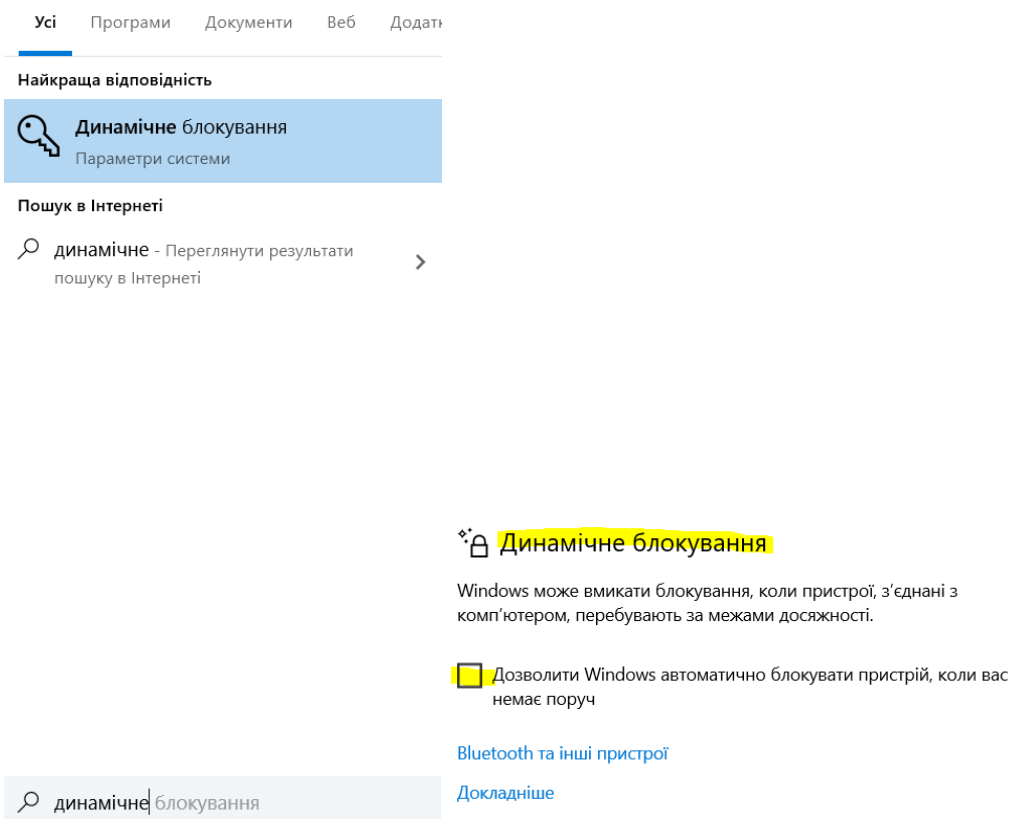
Налаштувати та перевірити роботу функції «Динамічне блокування» Windows, яка буде вмикати блокування, коли пристрої, з'єднанні з комп'ютером, опиняться за межами досяжності.

У смартфоні та комп'ютері включити Bluetooth, з'єднати пристрої між собою через відповідні налаштування Bluetooth (зобр. 2). Шляхом тестової передачі довільного файлу зі смартфона до комп'ютера переконатися у встановленому з'єднанні.



Зобр. 2. Підключення Bluetooth пристрою до комп'ютеру

На панелі задач у полі пошуку ввести запит «динамічне», обрати «Динамічне блокування» та ввімкнути «Дозволити Windows автоматично блокувати пристрій, коли вас немає поруч» (зобр. 3). Дочекатися, коли система знайде і відобразить графічно встановлене Bluetooth-підключення зі смартфоном.



Зобр. 3. Налаштування «Динамічне блокування» Windows

Розірвати з'єднання смартфона з комп'ютером, відключивши Bluetooth-адаптер смартфона, і дочекатися автоматичного блокування екрана (приблизно через 1 хвилину).

ПРАКТИЧНА ВПРАВА
«АВТОВІДТВОРЕННЯ ПІД ЧАС ПІДКЛЮЧЕННЯ ЗНІМНИХ НОСІЇВ»

Навчальна мета заняття: налаштувати блокування ОС Windows за відсутності активності.

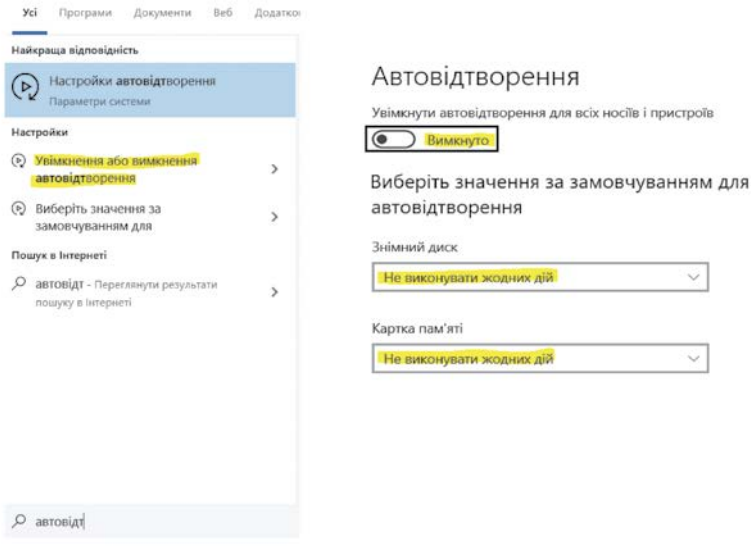
Час проведення: 0,1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Для захисту від так званого «стілеру» (stealer), який використовує для крадіжки даних функцію автовідтворення під час підключення знімних носіїв, вимкнути функцію автовідтворення в ОС Windows.

На панелі задач у полі пошуку ввести запит «автовідтворення», обрати «Увімкнення або вимкнення автовідтворення» та вимкнути цю функцію (зобр. 1).



Зобр. 1. Вимкнення функції автовідтворення для всіх носіїв і пристроїв

Підключити знімний носій до комп'ютера та переконатися у відсутності автоматичного відтворення змінного носія.

МОДУЛЬ № 8:

УБЕЗПЕЧЕННЯ ВІД НЕПРАВДИВИХ ПОВІДОМЛЕНЬ

ПРАКТИЧНА ВПРАВА

«ІНСТРУМЕНТИ ВИЯВЛЕННЯ НЕПРАВДИВИХ ПОВІДОМЛЕНЬ»

Навчальна мета заняття: навчитися перевіряти окремі відомості в мережі Інтернет на достовірність.

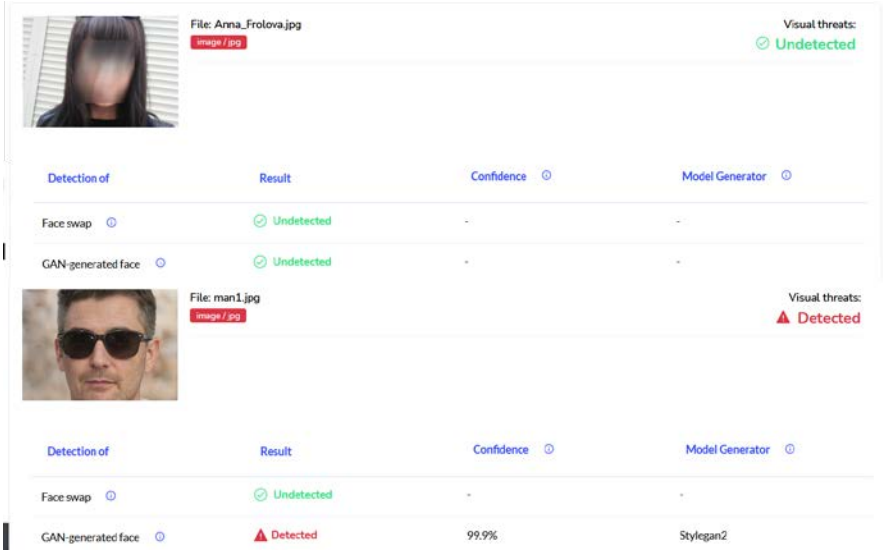
Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

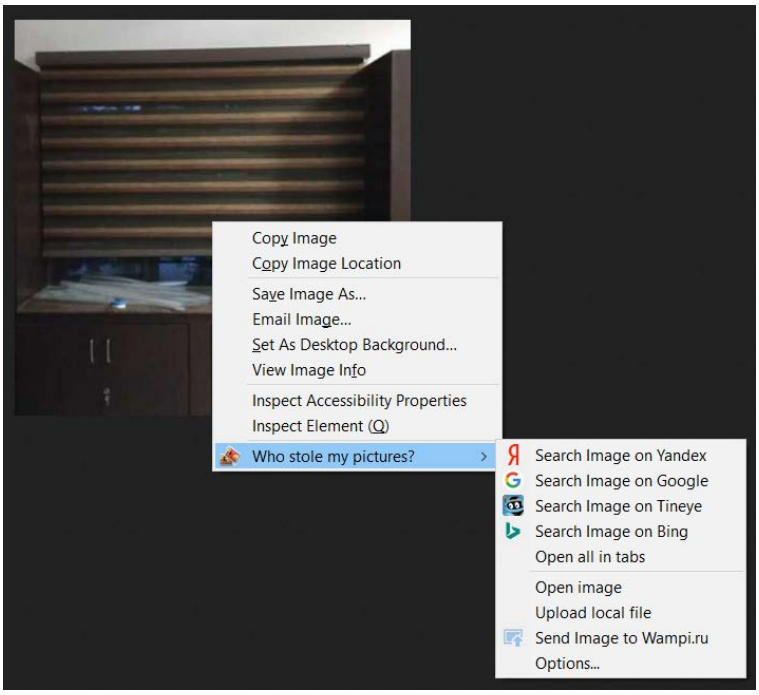
Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень. Серед подібних інструментів можна виділити такі.

Deepfake detection – це інструмент, який дозволяє виявляти підробку у різних мультимедійних файлах. Для використання цього продукту достатньо перейти за вказаним посиланням https://platform.sensity.ai/deepfake-detection#, авторизуватися. Після цього стають доступними функції завантаження мультимедійного документа для перевірки (зобр. 1).



Зобр. 1. Перевірка зображень на предмет маніпуляцій

Зображення можуть не мати ознак маніпуляцій, проте використовуватися у неправдивих повідомленнях у різних контекстах. Для того, щоб знайти першоджерело відповідних малюнків можна використовувати розширення Who stole my pictures (зобр. 2).



Зобр. 2. Використання розширення для пошуку зображень

Завантажити описане розширення можна за адресами:

- для браузеру «Chrome» (https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd);
- для браузеру «Firefox» (https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/).

1. Створіть декілька зображень за допомогою ресурсу thispersondoesnotexist.com, а також завантажте декілька медіафайлів із соціальних мереж.

2. Дослідіть роботу описаних програмних інструментів.

МОДУЛЬ № 9:

ПРАВОВІ ЗАСАДИ КІБЕРГІГІЄНИ

ПРАКТИЧНА ВПРАВА

«ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ»

Навчальна мета заняття: провести гру «Дебати» за темою для виявлення та закріплення знань.

Час проведення: 1 год. Місце проведення: навчальна аудиторія.

Устаткування: ручка, зошит.

Короткі теоретичні відомості

У контексті вивчення кібіргігієни працівниками органів державної влади та місцевого самоврядування потрібно розуміти окремі аспекти вітчизняного законодавства, яке має давні традиції унормування правил безпечної роботи з інформацією.

У національних нормативно-правових актах на сьогодні відсутнє безпосереднє згадування такої категорії як кібергігієна. Водночас найбільш дотичними термінами у досліджуваному контексті є «інформаційна безпека» та «кібербезпека».

Згідно зі статтею 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу.

25 лютого 2016 р. Указом Президента України № 47/2017 було затверджено Доктрину інформаційної безпеки України, в якій зазначено, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Інформаційна безпека та кібербезпека держави є складовою частиною її національної безпеки. В Україні питанню забезпечення національної безпеки традиційно приділяють велику увагу. Здійснивши екскурс в історію, можна побачити, що від самого початку становлення України як незалежної держави методично ухвалювалися нормативно-правові акти, які містили безпосередні вказівки для того чи іншого напряму забезпечення національної безпеки.

У зв'язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України», який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектору безпеки України.

Відповідно до п. 9 ч. 1 ст. 1 цього Закону, ***національна безпека*** – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз.

Складові частини національної безпеки можна представити як на зобр. 1.

Зобр. 1. Структура національної безпеки України

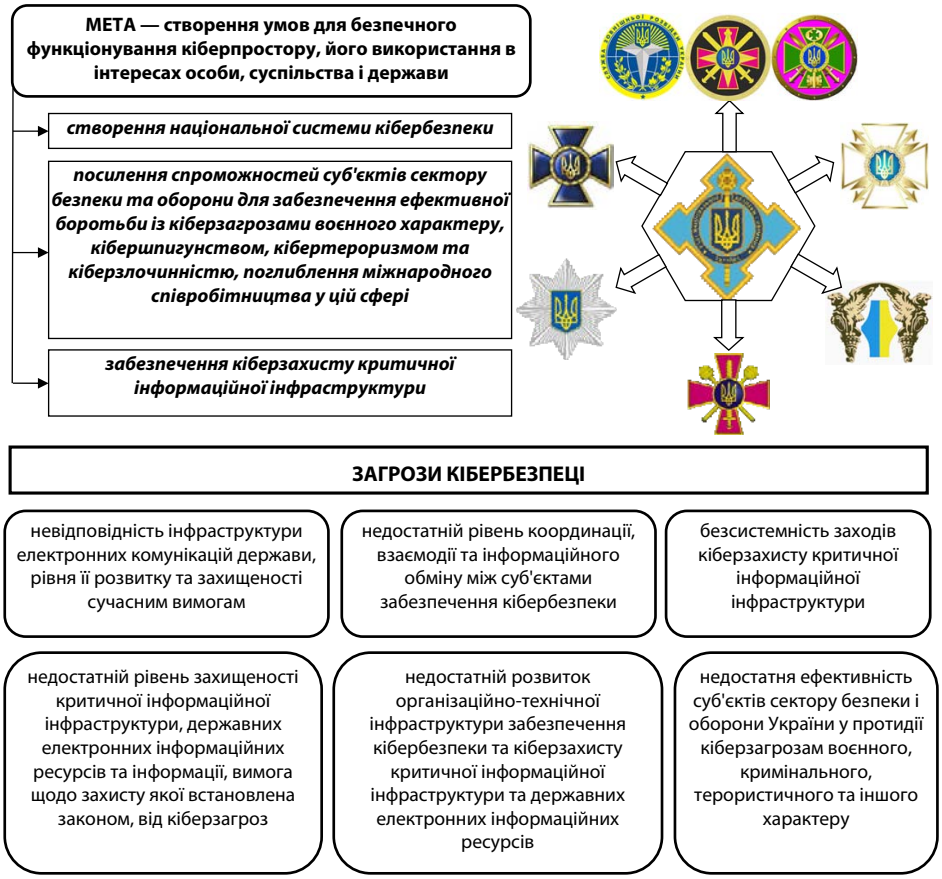
За вказаними напрямами безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно, в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо.

Окремим нормативним актом затверджено ***Стратегію кібербезпеки України*** – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Більш докладно структуру вказаного документа зображено на зобр. 2.

Слід наголосити, що в Законі України «Про національну безпеку України» не надається визначення термінів «інформаційна безпека» та «кібербезпека». На законодавчому рівні їх закріпили законами України «Про основні засади

забезпечення кібербезпеки України» від 05.10.2017 та «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007.

Зокрема, ***кібербезпека*** – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.



Зобр. 2. Основні елементи стратегії кібербезпеки України

Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

Кібергігієна є важливим елементом кібербезпеки, проте ці поняття не є тотожними. Якщо кібербезпека пов'язана з об'єктивним оцінюванням дій, спрямованих на підтримку безпеки та дотримання захисту від кібератак, то кібергігієна асоціюється зі знаннями про безпеку в Інтернеті та правилами покращення кібербезпеки[29]. Також кібергігієна передбачає дотримання правил поведінки, що стосуються інформаційної безпеки.

Згідно з п. 13 розділу III Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки під ***інформаційною безпекою*** розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам і забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній

[29] Neigel A. R., Claypoole V. L., Waldfogle G. E., Acharya S., Hancock G. M. Holistic Cyber Hygiene Education: Accounting for the Human Factors. *Computers & Security.* 2020. Vol. 92. 101731 (DOI: 10.1016/j.cose.2020.101731).

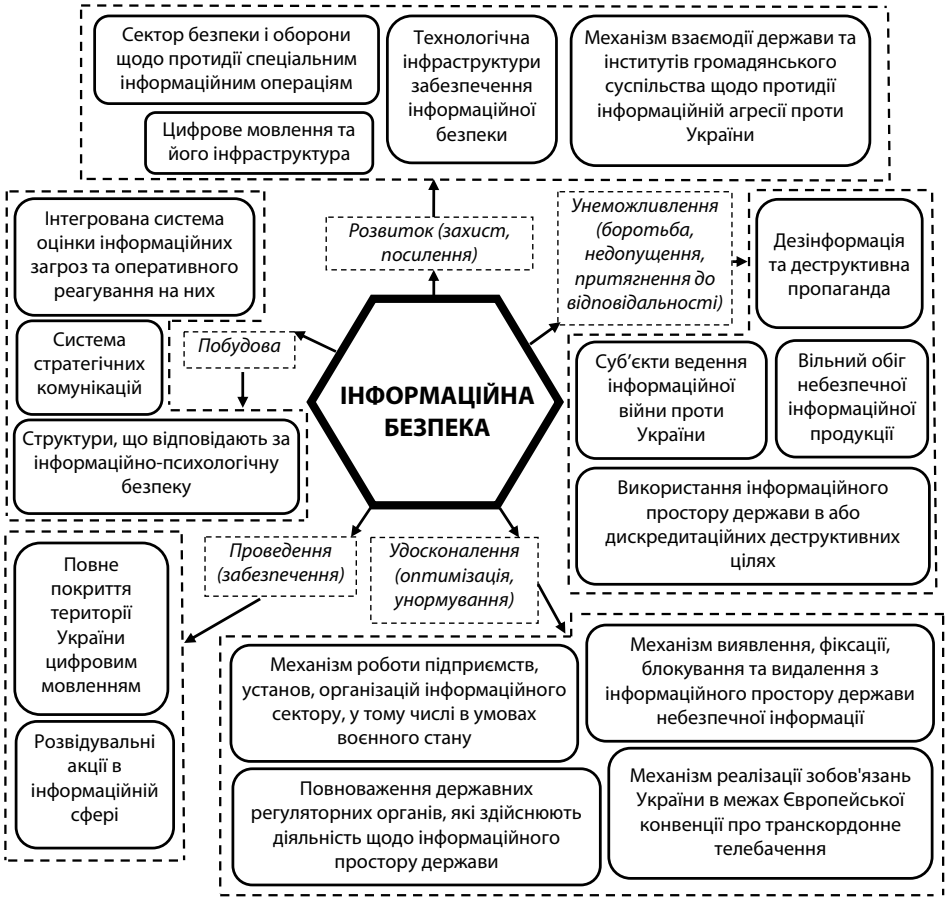
злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Виходячи зі змісту Доктрини інформаційної безпеки України, на зобр. 3 представлено основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки як складової національної безпеки України є:

- громадяни України та їх об'єднання;
- Верховна Рада України, яка, серед іншого, ухвалює закони у сфері інформаційної безпеки, визначаючи тим самим державну політику в цій сфері;
- Президент України, який забезпечує послідовне проведення державної інформаційної політики, інформаційний суверенітет та інформаційну безпеку України;
- Кабінет Міністрів України, який організовує діяльність виконавчої влади щодо забезпечення інформаційної безпеки;
- Рада національної безпеки і оборони України, яку очолює Президент України, координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки України;
- інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;
- засоби масової інформації та інші суб'єкти, які здійснюють інформаційну діяльність;
- наукові установи та навчальні заклади, які, серед іншого, проводять наукові дослідження та здійснюють підготовку фахівців з інформаційної безпеки.



Зобр. 3. Основні пріоритети забезпечення інформаційної безпеки

Залежно від конкретного виду інформації встановлюються різні рівні її захисту. Для визначення конкретних захисних механізмів використовується принцип поділу інформації за порядком доступу на відкриту та з обмеженим доступом. Загальна структура такого поділу наведена на зобр. 4.

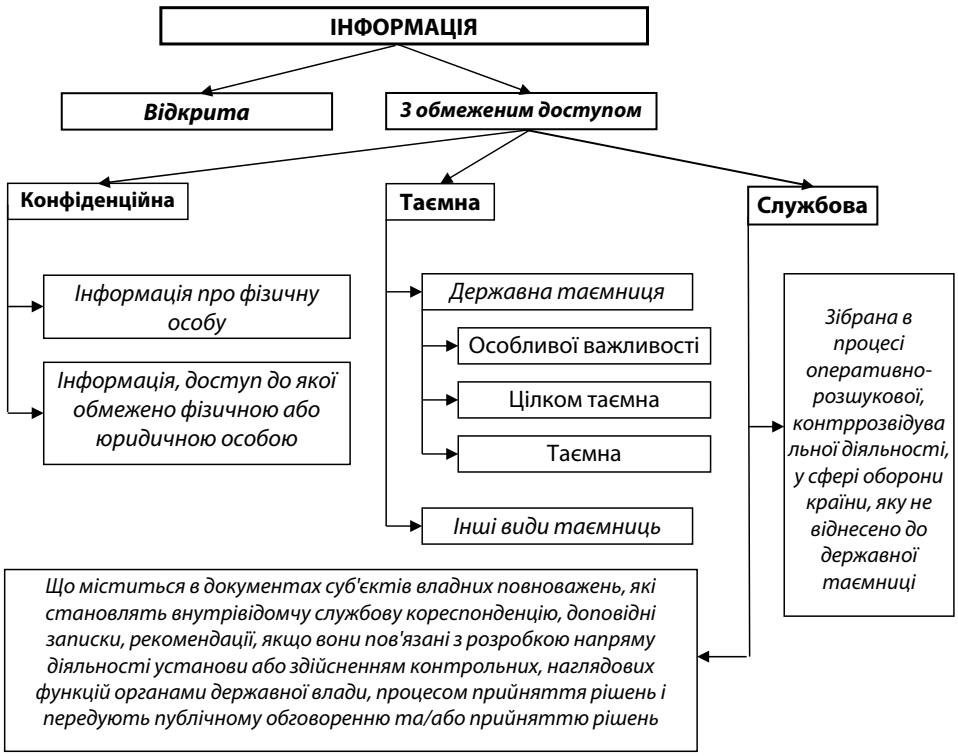
Захист відкритої інформації в державних органах регламентують:

1. Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 08.10.1997 № 1126[30].

[30] Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (дата звернення: 12.07.2017).

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373[31].

Захисту потребують такі властивості відкритої інформації, як *цілісність і доступність.*



Зобр. 4. Класифікація інформації за порядком доступу

Будь-яка інформація є **відкритою**, крім тієї, що віднесена законом до інформації з обмеженим доступом. До відкритої інформації, що підлягає захисту, відносять інформацію, яка належить до державних інформаційних ресурсів, а також про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами.

[31] Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями]. *Офіційний вісник України.* 2006. № 13 (12.04.2006), стор. 164, стаття 878.

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію»[32], ***конфіденційною*** є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи *у визначеному* нею *порядку* відповідно до *передбачених* нею *умов*, а також *в інших випадках, визначених законом*. Встановлення системи захисту є правом, а не обов'язком власника. Конфіденційна та службова інформація належать до інформації з обмеженим доступом, але не всяка інформація може бути визнана такою. Законодавець встановлює з цього приводу певні обмеження.

За розголошення конфіденційної інформації, що не є власністю держави, може наступати адміністративна відповідальність у порядку, визначеному ст. 164-3 Кодексу України про адміністративні правопорушення (КУпАП) від 07.12.1984. Крім того, адміністративна відповідальність може наставати також за порушення порядку використання конфіденційної інформації (ст. 186-3 КУпАП).

Більш урегульованими з правової точки зору є питання захисту службової інформації. Порядок ведення обліку, зберігання, використання та знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, детально прописаний у Типовій інструкції, затвердженій Постановою Кабінету Міністрів України від 19.10.2016 № 736[33].

За порушення роботи зі службовою інформацією передбачена адміністративна, а в окремих випадках – кримінальна відповідальність. Так, згідно зі ст. 212-5 КУпАП, порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних

[32] Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

[33] Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету міністрів України від 19.10.2016 № 736. *Офіційний вісник України*. 2016. № 85 (04.11.2016), стор. 102, стаття 2783.

мінімумів доходів громадян і на посадових осіб – від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян. Повторне вчинення правопорушення збільшує розмір штрафу.

Кримінальна відповідальність встановлюється за розголошення службової інформації (зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни) *нерезидентам* України (іноземним підприємствам, установам, організаціям або їх представникам) (ст. 330 Кримінального кодексу України).

Також належать до інформації з обмеженим доступом ***персональні дані*** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Наразі в Україні діє Закон України «Про захист персональних даних» від 01.06.2010, яким унормовано порядок роботи з інформацією, що містить персональні дані[34].

Таку інформацію можна поділити на:

- **загальну**, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до п. 3 ст. 296 Цивільного кодексу України допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо);
- **вразливі персональні дані (конфіденційна інформація про особу)**, що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до

[34] Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України.* 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997, *до конфіденційної інформації про особу*, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).

У 2012 році Конституційний суд України додатково розтлумачив, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовій, інтимній, товариській, професійній, діловій та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини[35].

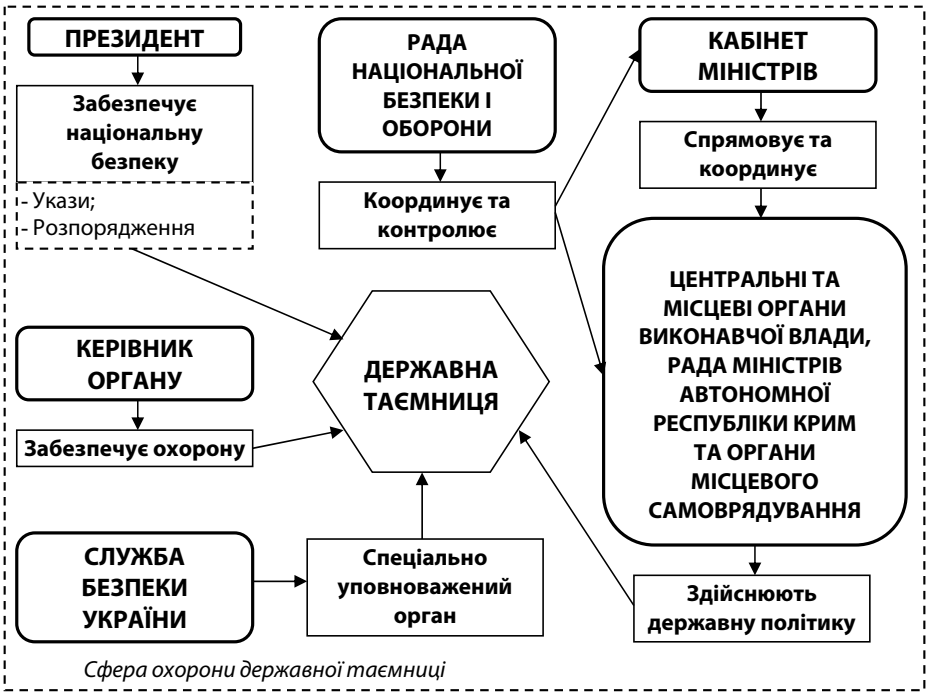
Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 № 373 та інших нормативних актів у сфері захисту інформації, **загальна інформація про особу**, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані –** як службова інформація, відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації, згідно з вимогами Закону України «Про захист персональних даних» від 01.06.2010.

[35] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. *Офіційний вісник України.* 2012. № 9 (10.02.2012), стор. 106, стаття 332.

Захист інформації, яка становить державну таємницю, регламентується, перш за все, Конституцією України, кількома міжнародними договорами, ратифікованими Верховною Радою України, Законом України «Про державну таємницю» від 21.01.1994[36], Кримінальним кодексом України та низкою підзаконних актів.

Згідно зі ст. 1 Закону України «Про державну таємницю», ***державна таємниця*** – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом, державною таємницею і підлягають охороні державою.

Організаційну структуру охорони державної таємниці умовно можна представити як на зобр. 5.



Зобр. 5. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

[36] Про державну таємницю: закон України від 21.01.1994; [із змінами і доповненнями]. *Відомості Верховної Ради України.* 1994. № 16 (19.04.1994). стор. 422. ст. 93.

За порушення законодавства про державну таємницю передбачена дисциплінарна, адміністративна (ст. 212-2 КУпАП) та кримінальна відповідальність (ст. ст. 111, 114, 328, 329, 422 Кримінального кодексу України).

Порядок проведення заняття

1. Слухачі заздалегідь отримують матеріали для підготовки та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є тренер).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього тренер ставить питання, номер якого відповідає названому доповідачами числу у списку питань тренера. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає, то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене тренером питання. У цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання тренера протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання відповідно до відповіді доповідачів.
6. Опоненти ставлять питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти ставлять питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Тренер ставить контрольне питання за розглянутим питанням кожній з команд.
11. Тренер оцінює якість роботи кожної з команд.

Критерії оцінювання (за п'ятибальною шкалою кожний):

- повнота та аргументованість відповідей;
- робота в команді;
- дотримання правил етикету.

12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченні гри підбиваються підсумки.

Follow OSCE Project Co-ordinator in Ukraine

Україна, 01030, Київ,

вул. Стрілецька, 16

info-pcu@osce.org

www.osce.org/ukraine

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні