Безпечне користування електронною поштою

План лекції

Вступ
1. Принцип роботи електронної пошти
2. Види атак
3. Загрози під час користування поштовою скринькою
Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

Кожного дня ми використовуємо електронну пошту в робочих та особистих цілях. Вона стала одним з основних каналів комунікації з нами, а відтак – неабияким чином привабливою для кіберзлочинців. Розглянемо, які існують загрози під час використання електронної скриньки, а також як від них захиститись.

1. Принцип роботи електронної пошти

Електронна пошта – сервіс Інтернет для передавання текстових повідомлень та прикріплених до них файлів у вигляді листів та відкладеного їх зчитування (рис. 1).

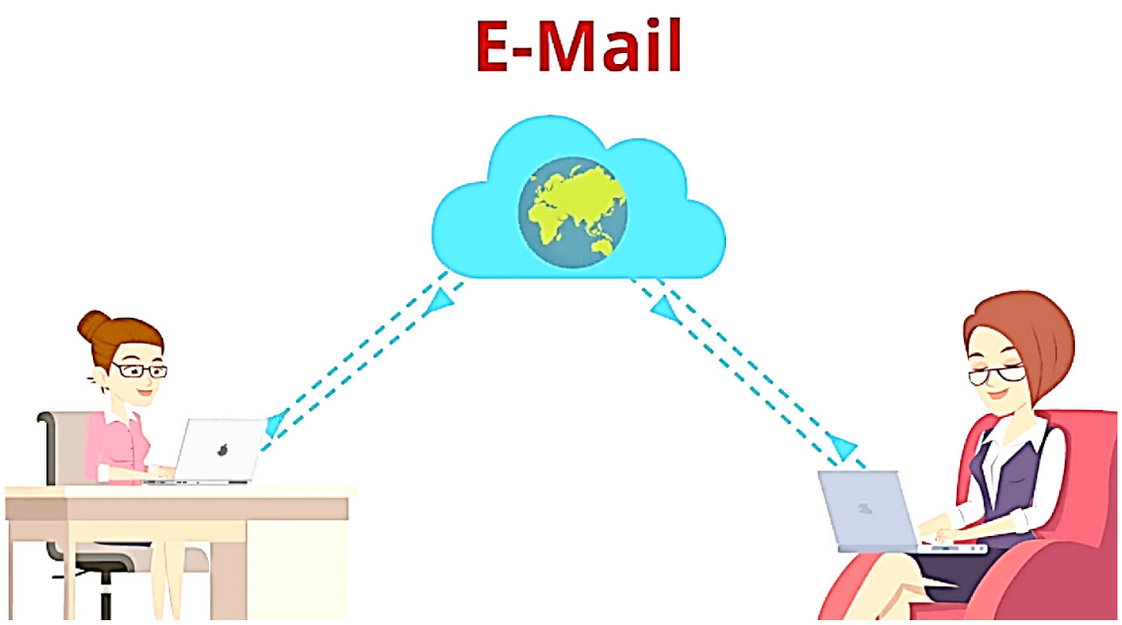

Рис. 1. Електронна пошта як сервіс передавання текстових повідомлень та прикріплених до них файлів з відкладеним зчитуванням (https://www.youtube.com/watch?v=VEYC1VnnEaY)

Розглянемо принцип роботи електронної пошти.

На рис. 2 показано типову послідовність подій, коли Аліса відправляє листа за допомогою поштової програми (клієнта) (Mail User Agent, MUA). Аліса вводить e-mail адресата та натискає кнопку «Відправити».

1. Поштовий клієнт форматує повідомлення в спеціальний формат та відправляє його за протоколом SMTP (Simple Mail Transfer Protocol) до агента з відправлення пошти (mail submission agent, MSA) на поштовому сервері smtp.a.org, де зареєстрована її поштова скринька.

2. MSA визначає адресу призначення, що фігурує у протоколі SMTP (а не в заголовку повідомлення), – bob@b.org. Назва перед @ – це локальна частина адреси, часто це – ім'я користувача / одержувача, а текст після @ – доменне ім'я. MSA надсилає запит до сервера системи доменних імен (DNS), щоб визначити доменне ім'я поштового сервера Боба.
3. DNS-сервер для домена b.org (ns.b.org) надсилає у відповідь MX-записи, в яких перелічено поштові сервери цього домена, зокрема mx.b.org – це поштовий сервер домена b.org.
4. Сервер smtp.a.org за допомогою протоколу SMTP надсилає лист на mx.b.org до кінцевого агента доставки повідомлень (message delivery agent, MDA), який доставляє його до поштової скриньки Боба.
5. Боб натискає кнопку «Отримати повідомлення» в поштовому клієнті, який отримує листи з сервера за протоколом Post Office Protocol (POP3) або Internet Message Access Protocol (IMAP).
6. MUA користувача bob забирає повідомлення за допомогою поштового протоколу (POP3) або протоколу доступу до інтернет-повідомлень (IMAP).

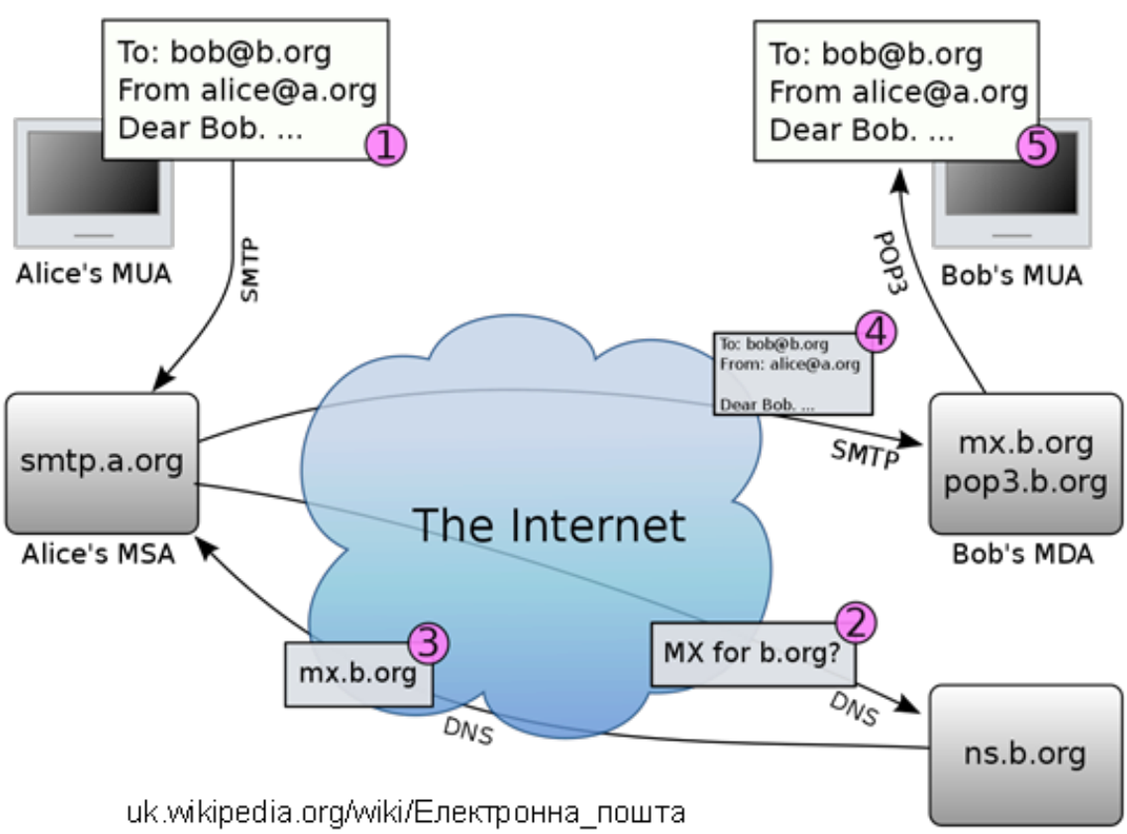

Рис. 2. Принцип роботи електронної пошти

Замість поштового клієнта користувачі часто використовують веб-браузер, який підключається до поштового сервера за протоколом https.

2. Види атак

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

- Вірус ***ILOVEYOU*** (2001) завдав збитків на суму близько 10 млрд дол. США. Було уражено ~10% всіх комп'ютерних систем у світі. Злочинці надіслали листи із зізнанням у коханні та скористались людською цікавістю, щоб адресати відкрили файл у вкладенні.
- ***Вірус MyDoom*** (2009) завдав збитків на суму близько 38 млрд дол. США. Користувачі отримували листа нібито з помилкою доставки імейлу до якогось отримувача, і деталі помилки знаходились у вкладенні листа.

Основним каналом доставки зловмисних повідомлень є електронна пошта (рис. 3).

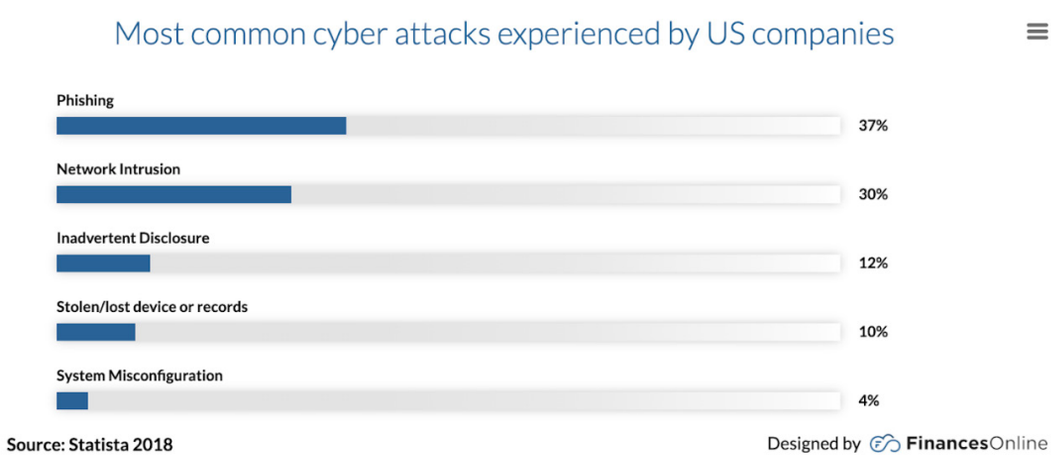

Рис. 3. Статистика атак за 2018 рік

Чому електронна пошта є настільки привабливою для кіберзлочинців?

- Бази даних поштових адрес відносно легко знайти в Інтернеті.
- Функція вкладень до листів дозволяє надсилати файли зі шкідливим програмним кодом.
- Користувачі не очікують отримати листи зі шкідливими вмістом.
- Користувачі часто несвідомо відкривають всі вхідні листи.

Особиста та робоча пошта

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

Службова пошта:

- показує вашу належність до організації – (vasyl@me.gov.ua). Ми бачимо, що Василь має відношення до Міністерства розвитку економіки. Одне це вже зумовлює довіру до листів, які надходять з цієї адреси;
- дані зберігаються на серверах вашої установи і керуються відділом інформаційних технологій. Треті сторони не мають доступу 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.

Отже, при використанні особистої та службової пошти не за призначенням:

1) ми 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 вашої скриньки;
3) збільшуємо ймовірність зламу ваших облікових записів.

Наслідком може бути те, що саме ваші облікові записи можуть стати інструментом для атаки на вашу організацію.

Як слід обирати поштовий сервіс для власного користування.

Необхідно зазначити, що провайдери поштового сервісу – це комерційні компанії, і вони потребують отримання доходу від своєї діяльності, тому:
«Якщо ми не платимо за продукт, ми є продуктом (в даному випадку – наші дані та інформація, яка проходить через нас)».

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».

Отже, коли ви обираєте поштовий сервіс, необхідно відповісти на питання: Чи готові ви платити за користування поштовим сервісом?

- якщо Так, тоді рекомендований сервіс: https://protonmail.com/ua/signup (є безкоштовна опція з лімітом на 500 Мб);
- якщо Ні, тоді ви будете платити вашими даними.

Якщо ви обрали все ж таки платити своїми даними, звертайте увагу на такі питання:

- з якої країни походить компанія?
- чи підвладна ця компанія державі?
- чи була помічена вона у витоках інформації про своїх користувачів?
- чи є політичний інтерес у цієї держави?

2. Загрози під час користування поштовою скринькою

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

Які мотиви зловмисника надсилати фішингові листи?

1. Отримати конфіденційні дані.
Злочинець надсилає лист з темою «Вас зламали! Швидше змініть пароль» і видає себе за авторитетне джерело – Google (рис. 4).

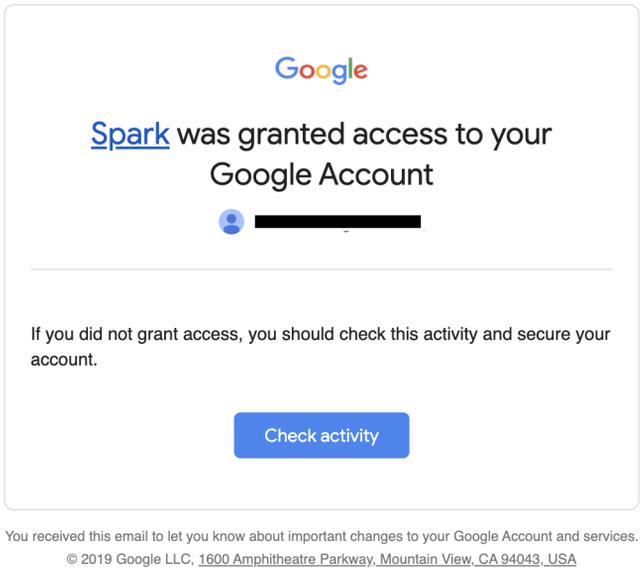

Рис. 4. Підроблений лист від Google

Мета листа – перехід за підробленим посиланням і підтвердження даних облікового запису через ввід паролю. Для цього створюється сайт, який буде майже не відрізнятись від справжнього (рис. 5).

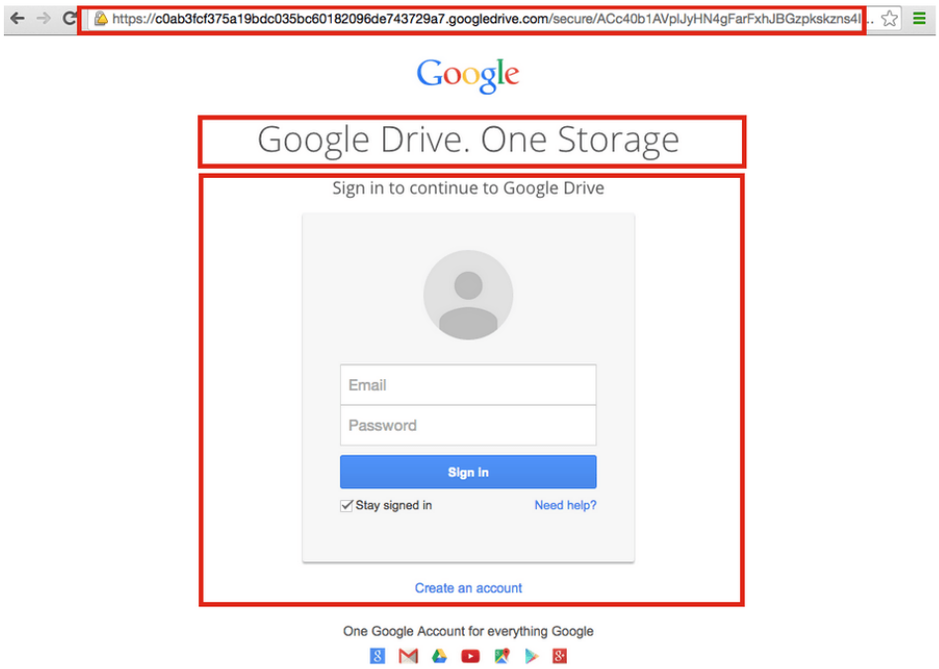

Рис. 5. Підроблений сайт автентифікації Google

Одержавши ваші конфіденційні 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 автентифікації. Адже якщо злодій отримає ваші дані для входу, йому буде необхідно ще мати секретний код, який генерується на вашому телефоні.
Інформація про фішингову атаку.

«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. Руйнування комп'ютерної системи/мережі організації.
Зловмисник надсилає листа і видає себе за авторитетне джерело. Його мета – щоб ви запустили файл у вкладенні.

Як тільки ви відкриєте файл, почнеться процес шифрування файлів системи з метою подальшого вимагання грошового викупу за ключі відновлення файлів.

Маючи доступ до вашого комп'ютера, зловмисники 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 (рис. 6).

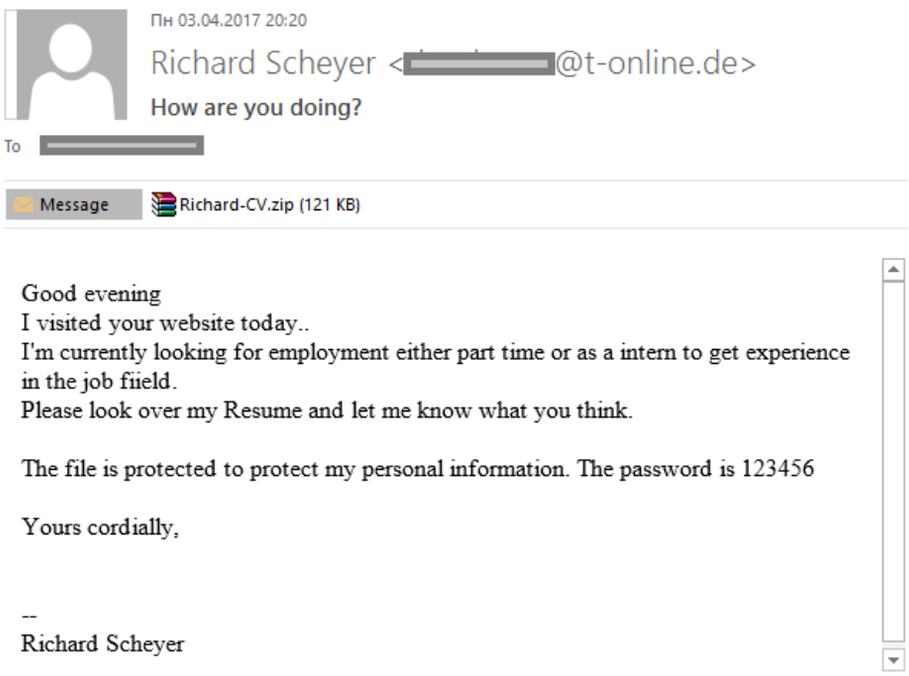

Рис. 6. Приклад листа із шкідливим вкладенням

3. Отримання віддаленого доступу до комп'ютера.

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, що надавало хакерам віддалений доступ для управління системою (рис. 7).

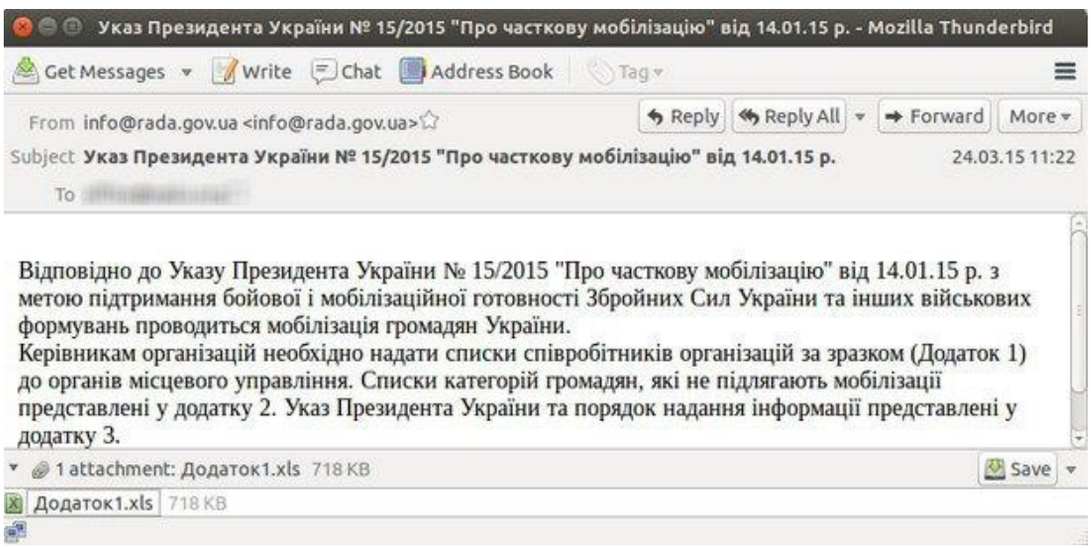

Рис. 7. Лист із ШПЗ

Злочинцям вдалось віддалено вплинути на роботу систем, а результатом цієї атаки стало:

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

Кіберзлочинці надсилають фішингові листи з метою:

- отримання доступу до облікового запису;
- шифрування файлів системи комп'ютера;
- отримання віддаленого доступу.

Як відрізняти легітимні листи від фішингових?

Переважна більшість фішингових листів є неочікуваними для отримувача. Перш ніж довіряти листу, необхідно здійснити аналіз заголовків (метаданих), змісту і вкладень листа.

Аналіз метаданих.

1. Звернути увагу на ім'я відправника, але воно може бути будь-яким, його легко підробити (рис. 8).

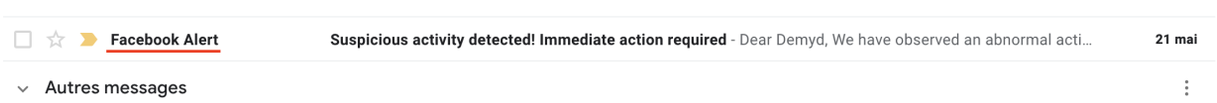

Рис. 8. Сумнівне ім'я відправника листа

2. Повідомлення, що закликає до швидких і термінових дій є індикатором фішингу, наприклад: «Вас зламали! Швидше поміняйте пароль за наданим посиланням».
3. Проаналізуйте правильність написання доменного імені відправника. Кіберзлочинці часто підмінюють літери/символи, щоб замаскуватись під авторитетне джерело. Так, accounts-google.com маскується під accounts.google.com

У 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».***

Іноді доменне ім’я відправника взагалі не маскується під легітимне (рис. 9).

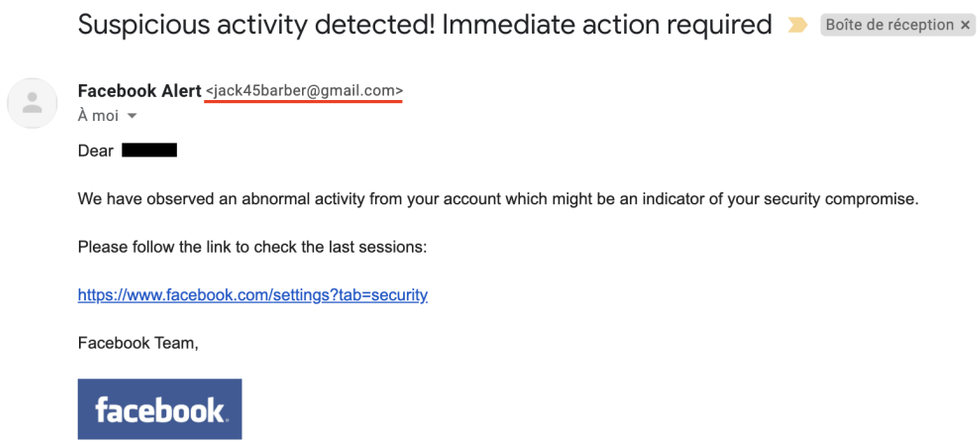

Рис. 9. Нерелевантне доменне ім’я відправника

Аналіз змісту повідомлення.

1. Звернути увагу на звернення: якщо використовуються загальні фрази «Шановні колеги», «Шановний клієнте» тощо, то у більшості випадків це – ознака фішингу (рис. 10). Злочинець може вказати ваше ім’я, тоді атаку можна вважати підготовленою спеціально під вас.

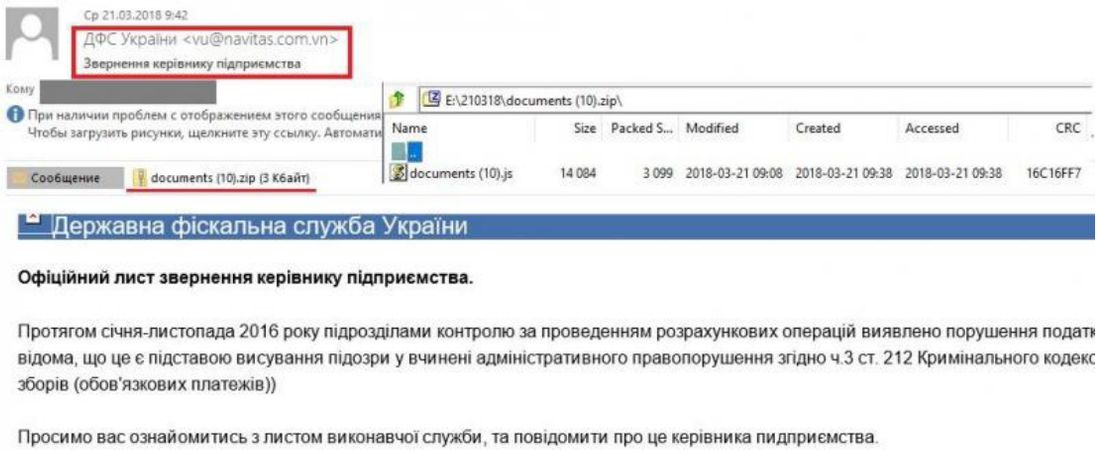

Рис. 10. Загальне звернення у листі

2. Невідповідна налаштуванням акаунту мова та наявність граматичних/орфографічних помилок є індикатором фішингового листа. Наприклад, Google надсилає листи, що стосуються облікового запису, мовою інтерфейсу цього запису. Тобто, якщо у вас інтерфейс українською мовою, а лист прийшов російською, це – серйозна причина задуматися.
3. Якщо файл у вкладенні зашифрований (архівований з паролем), а пароль зазначений у листі, то, скоріш за все, файл є шкідливим. Антивірусні системи поштових сервісів в цьому випадку не можуть виявити наявність ШПЗ у листі.

4. Необхідно здійснити аналіз активних посилань у листі. Обережно навести мишкою на посилання (не натискаючи) та потримати кілька секунд. У лівому куті буде відображено дійсне посилання (рис. 11).

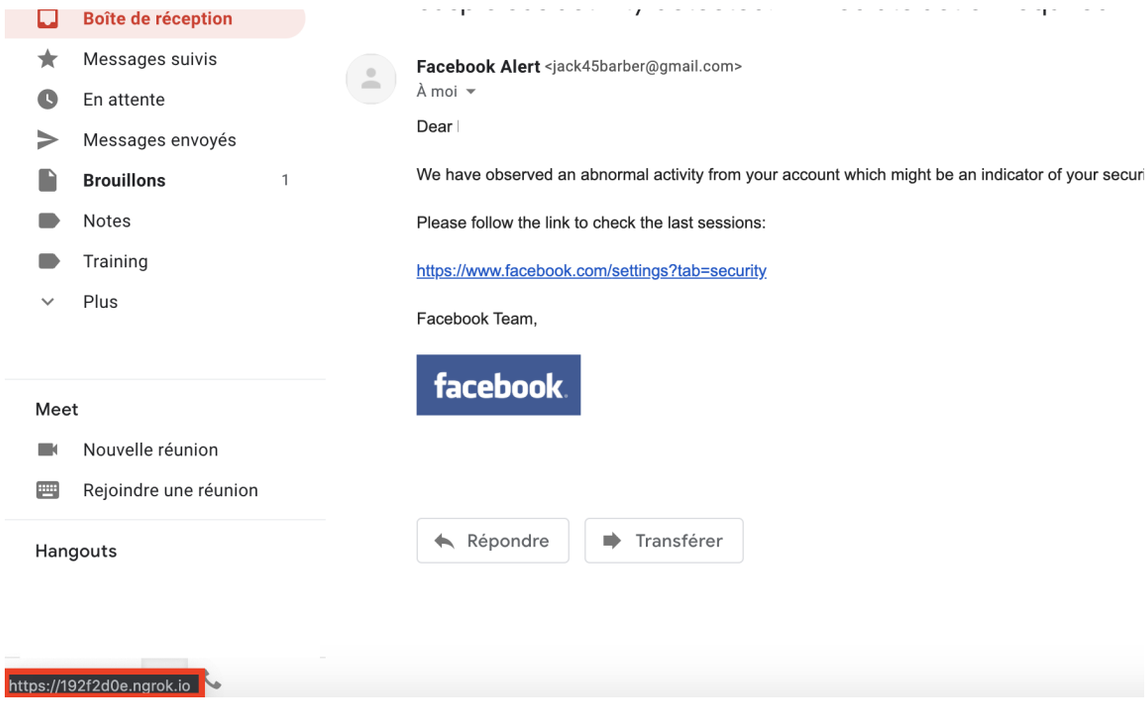

Рис. 11. Аналіз активного посилання у листі

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 вкладення.

Перелічені нижче файли можуть виконувати код в системі при їх відкритті і становити небезпеку:

- будь-які виконувані файли: EXE, COM, CMD, BAT, PS1, SWF, JAR, JS, VBS тощо;
- файли MS Office, особливо з макросами: DOC/DOCX/DOCM, XLS/XSLX/XLSM тощо;
- файли PDF;
- файли векторної графіки з вбудованим кодом: SVG;
- файли архівів, особливо з паролем: RAR, ZIP, 7Z тощо.

Висновки

Рекомендації із убезпечення поштового акаунту:

- використовувати складний пароль:
  - містить маленькі й великі літери, спеціальні символи та цифри, довжиною не менше 8–10 символів
  - перевірити складність паролю, який буде схожий на ваш: passwordmonster.com, www.security.org/how-secure-is-my-password;
  - не словникове слово, навіть модифіковане. Поганий пароль: rockandroll123. Складний пароль: T@8l3S0bk4hA7;
- зберігати складні паролі у парольних менеджерах;
- встановлювати двофакторну автентифікацію або passkey[13];
- не відкривати вкладені файли, не переконавшись у їхньому походженні:
  - для перевірки можна використовувати virustotal.com (в цьому випадку ви надаєте доступ до файлу третім особам);
- використовувати додатковий канал комунікації з тим, аби перевірити, чи дійсно надсилали вам цей лист (наприклад, за допомогою телефону, месенджера тощо);
- не використовувати службову пошту в особистих цілях;
- виходити з сеансу облікового запису;
- якщо у листі є скорочені посилання (https://bit.ly/xxxxx), перевірити їх можна через сервіси checkshorturl.com, expandurl.net.

Якщо все ж таки перейшли за посиланням у фішинговому листі, тоді:

- швидше змініть пароль;
- перегляньте відкриті сесії та закрийте ті, які вам не належать;
- зверніться до відділу IT-технологій.

Якщо відкрили вкладений файл і зрозуміли, що це був фішинг, тоді:

1) вимкніть комп'ютер;
2) зверніться до відділу IT-технологій.

13 https://en.wikipedia.org/wiki/Passkey_(authentication).