Тема 6.2 Принципи запровадження кіберкультури

6.2.1. Глосарій

Культура кібербезпеки - це набір припущень, уявлень, ставлення до предметної області, моделей поведінки та робочих звичок, які підсилюють кібербезпеку організації.
Кібергігієна - сукупність практик і підходів, які користувачі комп'ютерних систем застосовують для підтримки "здоров'я" та безпеки інформації в таких системах.
Анонімайзер - веб-сайт, який допомагає користувачу опосередковано отримати доступ до інших інтернет-сайтів, приховуючи свою особистість.
Правило порожнього робочого столу - під правилом порожнього робочого столу розуміють напрацювання звички не залишати жодні документи та цифрові носії інформації після завершення робочого дня або під час тривалої відсутності на безпосередньому робочому місці.
Фішинг - техніка, яка направлена на отримання чутливої інформації, наприклад, деталі банківських рахунків, персональних даних тощо, шляхом шахрайських дій і введення користувача в оману, використовуючи при цьому комунікацію через електронну пошту або веб-сайти, видаючи особистість відправника за вартий довіри контакт з робочого оточення чи бізнес-середовища.
Вішинг - це різновид фішингу, але контакт з користувачем встановлюється за допомогою засобів голосового зв'язку (дзвінок по телефону або засобами Інтернет-телефонії). Зловмисник представляється колегою з іншого відділу / співробітником технічної служби / діловим партнером або клієнтом. Часто такий різновид фішингу застосовується в комплексі з попередніми видами атак.

6.2.2. Вступ

Побудова системи кібербезпеки в організації передбачає ряд організаційних та технічних заходів, включно навчання і підвищення обізнаності серед широкого кола працівників організації. Саме недостатня обізнаність працівників і низький рівень загальної цифрової грамотності стає «слабким місцем» в системі кібербезпеки організації. Про це добре відомо зловмисникам, які «професійно» спеціалізуються на комп'ютерних злочинах. З іншого боку проінформований персонал створює перший ешелон захисту за допомогою дотримання простих повсякденних правил поведінки з інформацією в цифровому вигляді. Наявність спільного розуміння потреби в захисті інформації та знання простих правил для його підтримки – це ключові складові культури кібербезпеки в організації.

6.2.3. Поняття кібергігієни

Набір правил для повсякденної підтримки кібербезпеки для широкого кола працівників прийнято називати кібергігієною.

На рівні широкого кола користувачів наступні правила кібергігієни виділяють як найбільш важливі:

- правило чистого столу та екрану;
- правила роботи з паролями;
- правила безпечної роботи з електронною поштою;
- правила безпечної роботи з мережею Інтернет;
- правила використання флеш-накопичувачів та інших змінних носіїв інформації.

6.2.4. Правила роботи з паролями

Користування паролями є важливою складовою роботи з будь-яким програмним забезпеченням. Водночас паролі є невід'ємною частиною інформаційної безпеки. Вони забезпечують захист облікових записів користувачів, користувацьких даних і доступу до них. Використання слабкого пароля на робочому місці може призвести до того, що сторонні особи отримають доступ до даних пацієнтів або іншої важливої службової інформації.

6.2.4.1 Вимоги щодо створення паролів

З метою створення надійних паролів, які складно підібрати, слід ознайомитися з наступними вимогами.
Варто уникати паролей з однією або декількома ознаками, що наведені нижче.
Пароль вважається не надійним, якщо:

- для створення паролю використана інформація, яка прямо асоціюється з користувачем (власником паролю);
- в якості паролю обрано день народження, власний номер телефону або іншу персональну інформацію, яку можна порівняно легко дізнатися (наприклад, знайшовши інформацію в довідниках або в соціальних мережах, резюме, персональних оголошеннях тощо);
- в якості паролю обрано ім'я та/чи прізвище іншої людини (родича або знаменитості);
- в якості паролю обрано ім'я казкового персонажу;
- в якості паролю обрано кличку тварини, яка є популярною/розповсюдженою;
- паролем є назва юридичної особи, торгової марки, спортивного клубу чи музичного гурту;
- паролем є найменування сайту, апаратного або програмного забезпечення;
- пароль складається з одного словникового слова, яке застосовано без змін (написання слова відповідає написанню в словнику);
- пароль є регулярною послідовністю символів і цифр. Наприклад, 111111, abcde, qwerty;
- варіація перерахованих вище опцій, написаних у зворотному порядку;
- варіація перерахованих вище опцій, написаних із додаванням однієї цифри на початку або в кінці;
- варіація перерахованих вище опцій, написаних із додаванням одного знаку пунктуації;
- кількість символів в паролі недостатньо довга – сучасні дослідження доводять слабкість паролей довжиною меншою за 12 символів.

Примітка: Вимоги з вибору довжини паролю не менше 12 символів обумовлена наступними чинниками. В переважній більшості випадків для спроби підібрати пароль до облікового запису користувача, зловмиснику не потрібно знаходитися фізично біля робочого місця користувача. Також, зловмисники використовують високу ступінь автоматизації при підборі паролю. Спеціальне програмне забезпечення імітує дії користувача, перебираючи один можливий пароль за іншим упродовж днів, тижнів тощо. Окремі дослідження стверджують, що сучасні технології дозволяють порівняно швидко підібрати пароль, який має меншу довжину за 12 символів. Навіть, якщо всі інші рекомендації по вибору паролю враховано.

6.2.4.2. Поради по запам'ятовуванню складних паролів

Стійкий до підбору пароль має такі ознаки:

- містить як великі, так і малі літери;
- включає в себе декілька цифр;
- містить символи пунктуації або спеціалізовані символи (наприклад, % $ §* / &)
- має загальну довжину не менше 12 символів;
- не має ознак слабкого паролю, які було перераховано вище.

Хорошою практикою є вибір паролю, який одночасно є стійким до підбору і який можливо запам'ятати.

Одна з популярних технік для цього полягає в наступному. Пароль базується на довгій фразі, яку легко запам'ятати. Замість повних слів використовуються лише перші літери з кожного слова. Для стійкості в пароль додаються цифри та знаки пунктуації. Нижче наведено приклад:

Крок 1. Вибір фрази

The Beatles – Let it be

Крок 2. Вибір перших літер в словах

TBLib

Крок 3. Додавання цифр та знаків пунктуації

Отриманий пароль: TBLib-1970

Інша популярна техніка створення стійких паролів, які можливо запам'ятати, полягає в тому, щоб об'єднати в паролі декілька логічно не пов'язаних слів, змінивши їх написання і додавши цифри та спеціалізовані символи. Нижче наведено приклад:

Крок 1. Вибір довільних слів

хмарно мрія

Крок 2. Зміна написання слів

кмарно лрія

Крок 3. Додавання цифр та використання великих літер

кмаРно7 лРія2

Крок 4. Заміна окремих літер на символи, які схожі візуально

км@Рно7 лР!я2

Крок 5. Об'єднання окремих частин паролю

Отриманий пароль: *км@Рно7-лР!я2*

6.2.4.3. Рекомендації по використанню паролів

При роботі з паролями категорично **не рекомендується**:

- повідомляти пароль іншим особам, в тому числі особам, які представляються IT-спеціалістами;
- передавати особистий пароль колегам на час своєї відсутності, відпустки або відрядження;
- використовувати однаковий пароль для роботи та особистих цілей (напр., соціальні мережі);
- використовувати пароль, що схожий на попередній (при його зміні);
- використовувати пароль, який було надано адміністраторами – для первинного доступу до програмного забезпечення, без його подальшої безвідкладної зміни.

Примітка: Змінюйте паролі регулярно – принаймні один раз на рік для паролей від важливих службових програм, якщо частіший період не рекомендовано керівництвом закладу.

6.2.4.4 Рекомендації по зберіганню паролів

Якщо ви скористалися одним з вищенаведених методів по створенню пароля, який можливо запам’ятати, і у Вас є можливість відновити пароль через стандартний робочий процес – не записуйте пароль взагалі.
Якщо з певних причин пароль необхідно записати, **уникайте наступних сценаріїв**:

- ніколи не записуйте паролі на наліпках з подальшим розміщенням на моніторі або у блокноті, який зберігається прямо на робочому місці у відкритому доступі;
- не залишайте паролі в інших місцях, де з ними можуть ознайомитися сторонні люди;
- не зберігайте паролі в електронному вигляді у комп'ютері або смартфоні.

Примітка: Для зберігання паролів існує спеціалізоване програмне забезпечення, наприклад: KeePass https://keepassxc.org/ або 1Password https://1password.com/
Використання текстових редакторів та програм для нотаток загального призначення для зберігання паролів **категорично не рекомендується**.

6.2.4.5. Двофакторна автентифікація (2FA)

Двофакторна автентифікація (2FA) є процесом, що вимагає від користувача подання двох різних форм ідентифікації для отримання доступу до облікового запису. Це часто використовується як додатковий захисний етап для захисту ваших облікових записів і онлайн-сервісів. 2FA є важливою, оскільки вона додає додатковий рівень безпеки до вашого облікового запису, що ускладнює процес незаконного доступу. Навіть якщо зловмисник знає ваш пароль, він все одно не зможе увійти в систему, оскільки він потребує другого фактору автентифікації.
Як працює 2FA:
Двофакторна автентифікація працює шляхом використання двох з трьох можливих "факторів": щось, що ви знаєте (наприклад, пароль), щось, що ви маєте (наприклад, смартфон), або щось, що ви є (наприклад, ваш відбиток пальця). Деякі поширені приклади двофакторної автентифікації включають SMS-повідомлення з кодом, яке відправляється на ваш телефон після введення пароля, мобільні додатки, що генерують коди, та біометричні фактори, такі як відбитки пальців або розпізнавання обличчя.
Рекомендовані мобільні додатки для 2FA:

- Google Authenticator – це одна з найпопулярніших програм для двофакторної автентифікації, що створює коди автентифікації на вашому мобільному пристрої.
- Microsoft Authenticator – це інший широко використовуваний сервіс для двофакторної автентифікації, який також дозволяє використовувати багатофакторну автентифікацію.
- Authy – це служба двофакторної автентифікації, яка працює з багатьма веб-сайтами і сервісами. Authy надає різні опції для отримання кодів 2FA, включаючи SMS, дзвінки та мобільні програми.

Переваги 2FA:

- Збільшена безпека: додавання ще одного рівня автентифікації значно знижує ризик несанкціонованого доступу до облікового запису.
- Захист даних: 2FA є важливим інструментом для захисту вашої особистої та фінансової інформації.
- Зменшення шансів крадіжки ідентичності: навіть якщо ваш пароль став відомим, зловмисники все одно не зможуть отримати доступ до ваших облікових записів без другого фактора автентифікації.

Важливо пам'ятати, що 2FA є лише одним з компонентів загальної безпеки в Інтернеті. Це не повинно замінити інші важливі заходи безпеки, такі як використання складних паролів, регулярна зміна паролів і недопущення передачі своїх паролів іншим.

6.2.5. Рекомендації по безпечній роботі в мережі Інтернет

Мережа Інтернет надає безліч можливостей, але разом з тим, є місцем, де користувач ризикує зіштовхнутися з безліччю кіберзагроз. Якщо бути уважним та дотримуватися кращих практик безпечної роботи, можливо захистити себе від злочинців.

6.2.5.1. Підроблені веб-сайти

Зловмисники можуть різними способами заманити користувача на підроблений веб-сайт, який виглядатиме як точна копія оригіналу (копія порталу новин, соціальної мережі тощо). Головною відмінністю підробленого сайту буде його адреса. Але зловмисники намагатимуться зробити її дуже схожою на оригінал (наприклад, facelook.com, goooogle.com тощо).

6.2.5.2. Захищене підключення до веб-сайтів

Переважна більшість комерційних і майже всі державні веб-сайти забезпечують технологію захищеного інтернет-підключення. Для того, щоб користувач міг впевнитися в цьому, розробники популярних програм для перегляду інтернет-сайтів (так звані веб-браузери) виводять допоміжну інформацію поряд з адресою сайту, зазвичай у вигляді іконки замкненого замка.

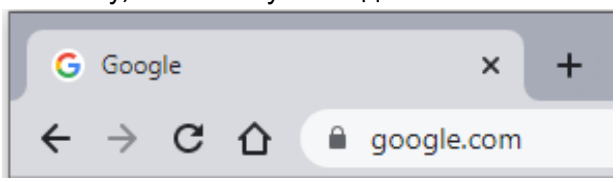

Рисунок 1. Іконка замкненого замка у веб-браузері Google Chrome

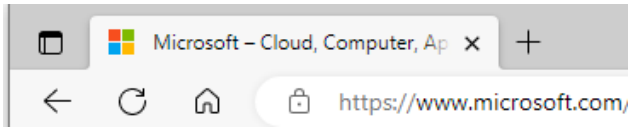

Рисунок 2. Іконка замкненого замка у веб-браузері Microsoft Edge

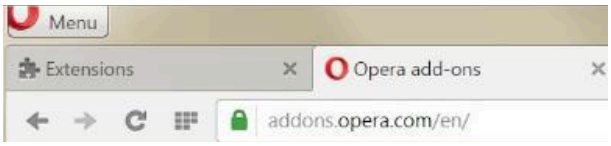

Рисунок 3. Іконка замкненого замка у веб-браузері Opera

Якщо немає впевненості, що сайт забезпечує технологію захищеного інтернет-підключення, будьте уважні і не вводьте жодні персональні, платіжні дані або пароль. Водночас захищене підключення ще не є гарантією того, що це не шахрайський сайт. Це значно ускладнює задачу створення шахрайського сайту, але не робить її неможливою.

6.2.5.3. Перевірка Інтернет-посилань

У разі сумнівів щодо надійності окремо взятого сайту можна скористатися безкоштовними Інтернет-сервісами для перевірки репутації того чи іншого веб-ресурсу. Розберемо цю задачу на прикладі сервісу Url Scan.

Крок 1. Скопіюйте адресу веб-сайту, репутацію якого треба перевірити, в «буфер обміну». Для цього виділіть текст адреси. Після чого, одночасно натисніть дві клавіші на клавіатурі: «Ctrl» та «c».

Крок 2. Відкрийте веб-сервіс Url Scan за допомогою посилання https://urlscan.io/ (див. рисунок 4)

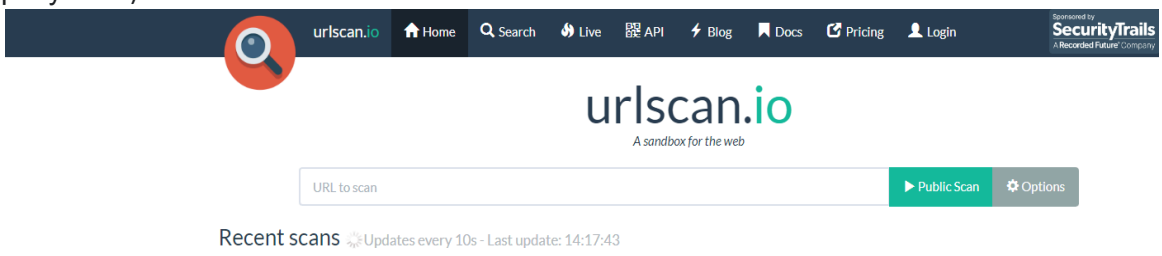

Рисунок 4. Фрагмент головної сторінки веб-сервісу Url Scan

Крок 3. Введіть адресу сайту у веб-сервіс Url Scan (див. рисунок 5)

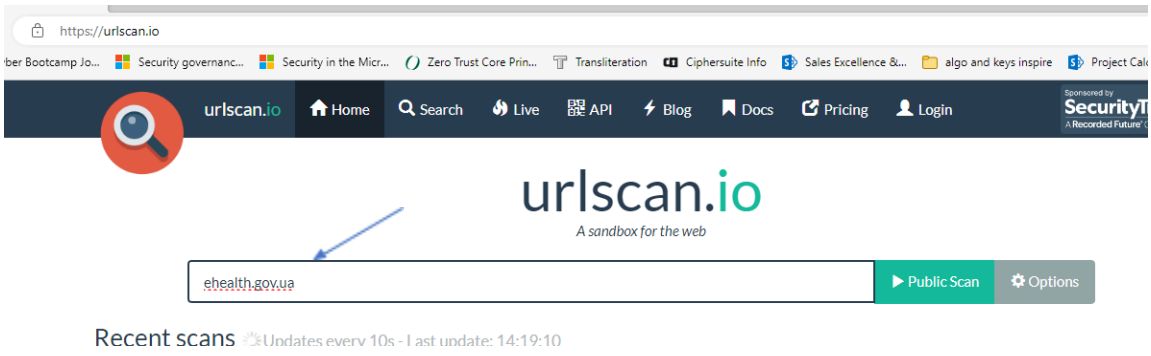

Рисунок 5. Перевірка адреси сайту у веб-сервісі Url Scan

Для цього, виконайте клік лівою клавішею мишки на полі для вводу адреси. Після чого, одночасно натисніть дві клавіші на клавіатурі: «Ctrl» та «v».

Крок 4. Натисніть зелену кнопку «Public Scan» (див. рисунок 6)

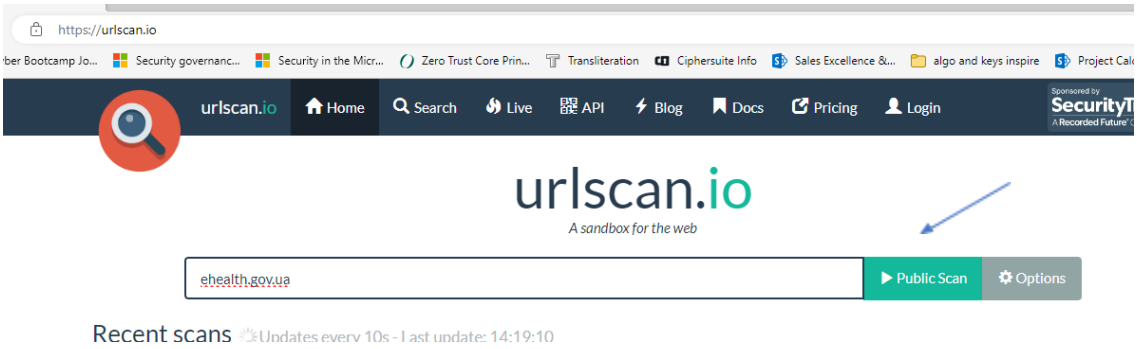

Рисунок 6. Перевірка адреси сайту у веб-сервісі Url Scan

Крок 5. Проаналізуйте аналіз сканування (див. рисунки 7-8)

Рисунки 7-8. Приклади результатів сканування

Ключовий рядок в результатах сканування – це «**urlscan.io Verdict**». У випадку, якщо на сторінці з результатами сканування у полі «urlscan.io Verdict» вказано значення **"malicious"**, використання даного веб-сайту несе **ризики** для Вашої кібербезпеки!

6.2.5.4. Рекомендації при роботі з веб-браузером

Популярні програми для перегляду інтернет-сайтів (так звані, веб-браузери) самостійно оновлюють себе для підвищення захисту від вірусів, без участі користувача. Тому, використання популярних веб-браузерів дає користувачу додаткову перевагу.

Будьте обережні при встановленні додаткової функціональності в браузерах, так званих add-on. Ці компоненти зазвичай є продуктами сторонніх розробників. В останніх можуть бути обмежені ресурси для підтримки їхньої безпеки та своєчасного випуску оновлень, порівняно з розробниками самих веб-браузерів. Вони можуть стати «слабким місцем» в безпеці роботи користувача в мережі Інтернет. Тому, не встановлюйте жодної додаткової функціональності в браузер, яка не потрібна для виконання робочих задач.

6.2.5.5. Рекомендації щодо використання проксі-ресурсів

Не рекомендується використання програмного забезпечення і веб-сайтів з метою приховування своєї діяльності в мережі Інтернет. До таких дій іноді звертаються працівники, які бажають використовувати службове Інтернет-з'єднання з робочого місця не за призначенням.

Веб-сайти «анонімайзери» зазвичай створюються та підтримуються шахраями з метою крадіжки паролів, а також персональних даних і фінансової інформації користувача. Навіть при використанні таких «анонімайзерів» без введення особистих даних на сайті, виникає ризик для всієї інформації, що зберігається на робочому комп'ютері та в робочій комп'ютерній мережі.

6.2.5.6. Рекомендації при роботі з Wi-Fi мережею

У випадку необхідності використання робочих систем за межами приміщень установи може постати потреба у підключенні до мережі Інтернет.
Категорично не рекомендується підключатися до публічних безпровідних Wi-Fi мереж, маючи на комп'ютері або смартфоні службову інформацію.
Це є дуже небезпечним сценарієм, оскільки більшість таких мереж не гарантують захист від копіювання інформації або її викривлення. Окремим сценарієм є випадки, коли зловмисники створюють шахрайські публічні точки доступу до мережі Інтернет через Wi-Fi мережу з метою крадіжки паролів і цінних даних. Такі мережі можуть мати назву кафе та інших закладів поблизу, що вводить користувачів в оману.
Кіберзлочинці налагоджують фейкові безпровідні точки доступу, що дає їм можливість перехоплювати конфіденційну інформацію, наприклад, банківські реквізити, дані платіжних карток тощо.
Щоб вберегти себе від проникнення злочинців до персональних даних через публічну Wi-Fi мережу, рекомендовано:

- вимкнути функцію автоматичного підключення до доступних безпровідних мереж;
- не виконувати робочі задачі та не вводити персональну чи платіжну інформацію при підключенні до мережі Інтернет через публічну Wi-Fi мережу.

6.2.5.7. Рекомендації по роботі з електронною поштою

Наступні рекомендації покликані **зменшити ризик витоку конфіденційних даних через кіберзагрози, пов'язані з використанням робочої електронної пошти:**

- не використовуйте корпоративну електронну пошту для відправки і отримання повідомлень, не пов’язаних із виконанням ваших посадових обов’язків. Також не використовуйте особисту пошту для робочого листування. Якщо не дотримуватися цього правила, Ви не можете бути впевнені, хто може мати доступ до ваших особистих і робочих даних. IT-відділ може бачити Вашу особисту переписку, а провайдери поштових сервісів — службову;
- бажано завести дві особисті поштові адреси для різних задач. Одну електронну пошту для підписок і реєстрацій в різних сервісах, іншу – для особистої переписки. Так адреса для особистої переписки не буде фігурувати в мережі Інтернет, а на Вашу особисту пошту буде приходити менше спаму;

- не зберігайте важливі документи в пошті довше необхідного часу – видаляйте їх після того, як потреба в них зникне;
- рекомендовано розглянути можливість використання програмного забезпечення для шифрування файлів перед відправкою електронною поштою за межі Вашої установи. Це застосовується для файлів з конфіденційною інформацією і в тих випадках, коли з отримувачем можна домовитися про такий порядок обміну файлами;
- остерігайтеся фішингових листів (див. розділ 6.2.5);
- прикладом широко доступного програмного забезпечення з можливістю шифрування є архіватори з функцією захисту архіву паролем. Вміст архіву в такому випадку шифрується. Прикладом є популярний архіватор WinZip. Варто зауважити, що використання цього методу без попереднього погодження з отримувачем може мати негативні наслідки. Отримання архівів з паролем є підозрілим вмістом і буде розцінено відповідним чином;
- остерігайтеся листів, що можуть містити файли зі шкідливим програмним забезпеченням.

Примітка. Найбільш ризиковані типи файлів, на які треба звертати увагу при роботі з поштою:
- архіви файлів, особливо захищені паролем. Популярні розширення архівних файлів: .sfx, .zip, .7z, .rar;
- файли, які є програмним забезпеченням, наприклад, файли з розширенням .exe, .com, .cmd, .bat, .ps1, .swf, .jar, .js, .vbs;
- документи, що містять макроси, наприклад, файли з розширенням .docm, .xlsm, .pptm;
- файли векторної графіки з вбудованим кодом: .svg.

Перш ніж відкривати вкладений файл, перевірте файл на спеціалізованих публічних сервісах, наприклад: https://virustotal.com/. Даний веб-сайт пропонує можливість завантажити файл для перевірки його безпечності. Веб-сайт має безкоштовну функціональність, яка доступна без реєстрації.

6.2.5.8 Правило порожнього робочого столу

Метою зазначеного правила є запобігання сценарію, коли з конфіденційним службовим документом ознайомиться особа, яка має фізичний доступ до Вашого робочого місця, але не має права доступу до документу, який лежить на столі. Прикладом такої особи може бути працівник, який прибирає приміщення або навіть сторонній відвідувач.
Похідним від правила порожнього робочого столу є правило порожнього екрану, яке передбачає закриття програм та електронних документів у Вашому робочому комп'ютері після завершення роботи з ними.

6.2.6. Фішинг як одна з найпоширеніших загроз інформації

6.2.6.1. Поняття фішингу

У кожному секторі економіки і в кожній країні працює правило: “користувач – це найбільш вразлива ланка ланцюга захисту інформації в організації.” Широке коло користувачів, професія яких не пов'язана безпосередньо з комп'ютерними технологіями, має обмежені знання про кіберзагрози інформації. Організована кримінальна спільнота, навпроти – має доступ до високо-технологічних інструментів і методик для скоєння комп'ютерних злочинів. В цих умовах постає гостра потреба в підвищені обізнаності медичних працівників з питань кібербезпеки.

Окрім технічних засобів, зловмисники активно використовують проти користувачів психологічні маніпуляції. Вони націлені на вразливість людини – довірливість, необачність, схильність до нелогічних дій у стані паніки або обурення. Цим психологічним прийомам сотні років, проте сьогодні з ними можна зіштовхнутися при роботі з комп'ютером, а не при живому спілкуванні. В таких умовах користувач вважає, що знаходиться в контрольованому та безпечному середовищі, і проявляє меншу обережність.

Серед вищезгаданих методів маніпуляції превалює «фішинг». Термін має англомовне походження – від англ. “рибалка”. Зазвичай жертва отримує “приманку” та “клюнувши на неї” виконує дії, на які розраховує зловмисник. Результатом цих дій зазвичай стає отримання зловмисником конфіденційної інформації. Контакт із жертвою зазвичай встановлюється через електронну пошту, соціальні мережі або месенджери.

Як було зазначено, кінцева мета фішингу – це отримання конфіденційних даних. Нижче наводиться короткий огляд інформації, яка є пріоритетною для зловмисників.

6.2.6.2. Дані, за якими «полюють» зловмисники

У більшості випадків зловмисників найбільше цікавить наступна інформація закладів охорони здоров'я:

- списки імен, адреси електронної пошти, номери мобільних телефонів пацієнтів та адреси проживання;
- інформація про стан здоров'я та призначене лікування пацієнтів – особливо цінною є інформація, яка впливає на рішення суду (наприклад, психічний стан пацієнта) або факти, якими можна легко шантажувати пацієнта (наявність хвороби, яку негативно сприймає соціум – ВІЛ, наркоманія та інше);
- списки імен і посад співробітників, організаційна структура закладу, телефони співробітників (в тому числі, внутрішні телефонні номери);
- технічні засоби і програмно-апаратне забезпечення закладу;
- інформація про підрядників закладу;
- вся інформація, що Ви публікуєте особисто або Ваші друзі/колеги публікують про Вас у мережі Інтернет, може бути використана зловмисникам проти Вас. Чим більше інформації має злодій, тим вища ймовірність успіху в реалізації злочину.

6.2.6.3. Рекомендації по боротьбі з фішингом

Наступні рекомендації направлені на протидію фішингу через канал електронної пошти.
Необхідно відноситися з особливою обережністю та недовірою до електронних листів, які мають наступні ознаки:

- лист від невідомого відправника;
- лист від відомого відправника, але з поштової адреси, яка відрізняється від попереднього листування (зокрема, частина адреси після символу @). Звертайте особливу увагу на листи від відправників, адреса яких не закінчується на .ua (реєстрація адреси в Україні);
- терміновість – фішингові повідомлення часто закликають до швидких дій, залишаючи менше часу на роздуми. Часто автор листа видає себе за керівний орган або підрозділ для підвищення відчуття терміновості;

- помилки в тексті або незвична побудова фраз – часто злочинці не говорять українською і використовують перекладачі;
- повідомлення, що написано іноземною мовою;
- пропозиція, від якої важко відмовитися – рекламні повідомлення дуже часто є фішинговими;
- лист з інтригуючою інформацією, який начебто помилково потрапив до Вас, наприклад, зарплатна відомість керівника, список працівників, запропонованих до підвищення тощо;
- листи, в яких не згадується Ваше імя, які не адресовані особисто Вам, проте написані по шаблонній формі, наприклад, «Шановний клієнт» тощо;
- текст підпису з контактами відправника в кінці листа не відповідає фактичному відправнику листа або його поштовій адресі;
- запит на надання особистої інформації, в тому числі, шляхом запрошення до заповнення онлайн-форм через веб-посилання в листі;
- лист, який містить вкладені файли;
- лист, який пропонує перейти за посиланням або натиснути курсором “мишки” на зображення в електронному листі.

До підозрілих листів застосовуйте правило 30 секунд (див. розділ 6.2.5.4 Правило 30 секунд).

6.2.6.4. Правило 30 секунд

Якщо лист викликає підозри, дайте собі 30 секунд на аналіз, не реагуйте на лист протягом цього часу. Від того, наскільки уважними Ви будете, залежить, чи втратите Ви свою інформацію, чи ні.
Не поспішайте відкривати приєднані до електронного листа файли або переходити за посиланням в тексті листа.
У випадку сумнівів запитайте поради у керівника чи IT спеціаліста Вашої установи.
Якщо лист надіслано від знайомого відправника, але має ознаки підозрілого – зв'яжіться з відправником альтернативним каналом зв'язку для підтвердження, що лист надіслав дійсно він.

6.2.6.5. Перевірка Інтернет-посилань в електронному листі

Перед відкриттям інтернет-посилання підведіть мишку до посилання, не натискаючи курсором на нього. Ви побачите спливаючий рядок зі справжнім інтернет-посиланням, яке може відрізнятися від тексту посилання, яке Ви бачите спочатку в листі. Підведіть курсор та оцініть, чи не викликає адреса у Вас підозри.
Наприклад, посилання мало б перевести Вас на сайт української державної установи. При цьому справжня адреса посилання містить сайт, який завершується на “.ru”, отже велика ймовірність, що це фішинг.
Перш ніж переходити за посиланням, Ви також можете скористатися перевіркою репутації веб-сайту (сайт з безкоштовною функціональністю, доступний без реєстрації):

https://urlscan.io/ — перевірка інтернет-посилання на шкідливий вміст.

Детальніше питання розкрито в розділі 6.2.4.3 Перевірка Інтернет-посилань.

6.2.6.6. Протидія психологічній маніпуляції під час фішингу

Знання того, які сценарії шахрайства можливі, значно підвищує стійкість користувача до них. Нижче наведено важливі емоційні стани, які зловмисники намагаються викликати у користувача для власних цілей:

1. **Почуття відповідальності перед керівництвом**: співробітник більш охоче йде на співпрацю зі зловмисником, якщо той повідомляє про «термінове доручення від керівництва».
2. **Страх:** страх провинитися перед керівництвом або страх перед комп'ютерними технологіями і небажання розбиратися в рекомендованих підходах до роботи з комп'ютером може підштовхнути користувача до необдуманого кроку.
3. **Сором:** сором зізнатися в недостатності комп'ютерних знань і, як результат, несвоєчасне звернення за кваліфікованою допомогою.
4. **Доброта:** надмірна доброта і альтруїзм можуть спонукати людину надати допомогу, поступаючись звичайними правилами безпеки або втрачаючи пильність.
5. **Цікавість:** ще одне дуже вразливе місце, адже кому буде не цікаво подивитись на помилково відправлену вам зарплатну звітність або фотографії з корпоративної вечірки, на яку ви не змогли потрапити?

Для досягнення поставленого результату зловмисники можуть вдаватися до таких технік:

- представлятися іншою особою;
- відволікати увагу;
- нагнітати психологічну напругу.

У разі виявлення підозрілого листа одразу зверніться до Вашого керівника та/або до IT-фахівців, які обслуговують Вашу організацію.

6.2.6.7. Інші різновиди маніпуляцій

Окрім методу фішингу через канал електронної пошти, зловмисники застосовують інші канали та методи, що описані нижче.
Один з них «вішинг» — від англ. „voice“ та „fishing“.

шою технікою, яка вимагає доступу зловмисника до фізичного місця роботи користувача, є «підкидання» флеш-накопичувача зі шкідливим вмістом.
Зазвичай, це робиться на вході до будівлі організації. Зловмисники хочуть створити видимість, що флеш-накопичувач загубив хтось із персоналу організації. Іншими популярними місцями є парковки, столові, вбиральні та робочі місця співробітників. На жаль, працівники закладу не завжди можуть бути впевнені в тому, що пацієнт, який зайшов до їхнього кабінету, не є зловмисником.

Коли співробітники організації знаходять подібний флеш-накопичувач, вони або бажають його присвоїти, або знайти володаря. В обох сценаріях співробітник забажає перевірити вміст флеш-накопичувача, для чого під’єднає його до комп'ютера. Саме цієї поведінки очікує зловмисник. Флеш-накопичувач містить шкідливе програмне забезпечення. В найгіршому випадку це програмне забезпечення зможе приховано контролювати комп'ютер або знищити всю інформацію на ньому.

Для того, щоб співробітник не став чекати повернення додому, а застосував флеш-накопичувач саме в робочий комп'ютер, зловмисники вдаються до додаткових хитрощів. Наприклад, наносять на флеш-накопичувач напис “Бухгалтерія” або “Зарплатна відомість”.

Ключові слова / теги

Культура кібербезпеки, кібергігієна, пароль, Інтернет, підроблені веб-сайти, перевірка веб-сайтів, анонімайзер, VPN, WI-FI, email, електронна пошта, фішинг, вішинг