КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.13.615
УДК 004.056

Якименко Юрій Михайлович
кандидат військових наук, доцент
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Рабчун Дмитро Ігорович
кандидат технічних наук
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

Запорожченко Михайло Михайлович
асистент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

МІСЦЕ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ПРОБЛЕМІ ВИТОКУ ДАНИХ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАХИСТУ КОРПОРАТИВНОГО СЕРЕДОВИЩА ВІД ФІШИНГОВИХ АТАК З ВИКОРИСТАННЯМ ЕЛЕКТРОННОЇ ПОШТИ

Анотація. Оскільки за останні два роки спостерігається тенденція до стрімкого зростання кількості та частки фішингових атак на співробітників компаній та звичайних користувачів, стає необхідним висвітлення питання захисту від такого різновиду атак соціальної інженерії. В умовах пандемії зловмисники знаходять все більше нових способів обману, тож навіть досвідчені користувачі мережі Інтернет можуть стати жертвою шахраїв.

Через те, що електронна пошта використовується майже в усіх компаніях, саме з її використанням проводиться більша кількість атак. У статті розглядаються основні методи, які використовують зловмисники при проведенні фішингових атак з використанням електронної пошти, ознаки того, що користувач став жертвою соціальних інженерів, та наведені рекомендації, як можна підвищити стійкість корпоративного середовища до подібних атак за допомогою організаційних методів.

Оскільки користувач є основою мішенню при проведенні фішингових атак, а вбудовані в браузер та поштовий клієнт інструменти в більшості випадків не забезпечують надійний захист від фішингу, саме користувач становить найбільшу небезпеку для компанії, оскільки він, ставши жертвою фішингової атаки, може через свою недостатню компетентність завдати компанії значних збитків. Саме тому обов'язково необхідно проводити навчання та періодичне тестування персоналу на предмет стійкості до цільових фішингових атак. Співробітники компанії повинні на практиці бути ознайомлені з ознаками фішингу, прикладами таких атак, принципами роботи з корпоративними даними та їх відповідальністю. Керівництвом компанії повинні бути створені та доведені до персоналу регламенти та інструкції щодо зберігання, обробки, розповсюдження та передачі інформації третім особам. Також співробітники повинні доповідати службі безпеки компанії про підозрілі листи, повідомлення, дзвінки чи осіб, які намагалися вивідати цінні дані. Підвищення загальної обізнаності за допомогою практичного навчання дозволить скоротити кількість інцидентів інформаційної безпеки внаслідок фішингових атак.

Ключові слова: кібербезпека; соціальна інженерія; фішинг; електронна пошта.

ISSN 2663 - 4023

ВСТУП

Сьогодні інформація в сфері IT та в інших сферах дуже часто має високу цінність для бізнесу, адже вона є одним з основних факторів, від якого залежить чи буде успішною компанія, як вона буде розвиватися, її репутація та безпека клієнтів. Однак кожна система, яка тим чи іншим чином пов'язана з отриманням, зберіганням і обробкою даних, завжди містить в собі слабку ланку – людину. Саме завдяки такому недоліку кіберзлочинці можуть не витрачати час і зусилля на подолання складних механізмів захисту, а спробувати застосувати прийоми соціальної інженерії для отримання конфіденційних даних компанії через її співробітників або пов'язаних з нею осіб. Кіберзлочинців, які застосовують прийоми соціальної інженерії на практиці, також називають соціальними інженерами.

Соціальна інженерія використовує слабкості людини, які включають в себе особистісні та професійні. До особистісних якостей можна віднести людську наївність, довірливість, співпереживання, страх тощо. Професійні ж якості пов'язані з компетентністю людини. До них можна віднести відсутність у працівника необхідних знань або ж невміння застосовувати їх на практиці, ігнорування посадових обов'язків, інструкцій компанії тощо. Через такі слабкості людина вважається найбільш вразливою ланкою, яка є найменш стійкою до зовнішнього впливу.

Постановка проблеми. Згідно зі звітом Verizon про розслідування витоків даних за 2021 рік (Verizon's 2021 Data Breach Investigation Report) [1], соціальна інженерія продовжує набувати тенденції до зростання, яка пов'язана з тим, що, по-перше, все більше кіберзлочинців усвідомлюють ефективність такого виду атак, а по-друге, протягом пандемії з'являється все більше різновидів шахрайства на тему COVID-19: від фішингових листів, в яких зловмисники намагались обманути жертву, видаючи себе за Всесвітню організацію охорони здоров'я, до різних видів шахрайства з вакцинами. Тож вже протягом двох років фішинг – один з різновидів соціальної інженерії – залишається одним із найпоширеніших варіантів злому та став причиною 36% витоку даних у 2020 р. (рис. 1), що на 11% більше, ніж у 2019 р.

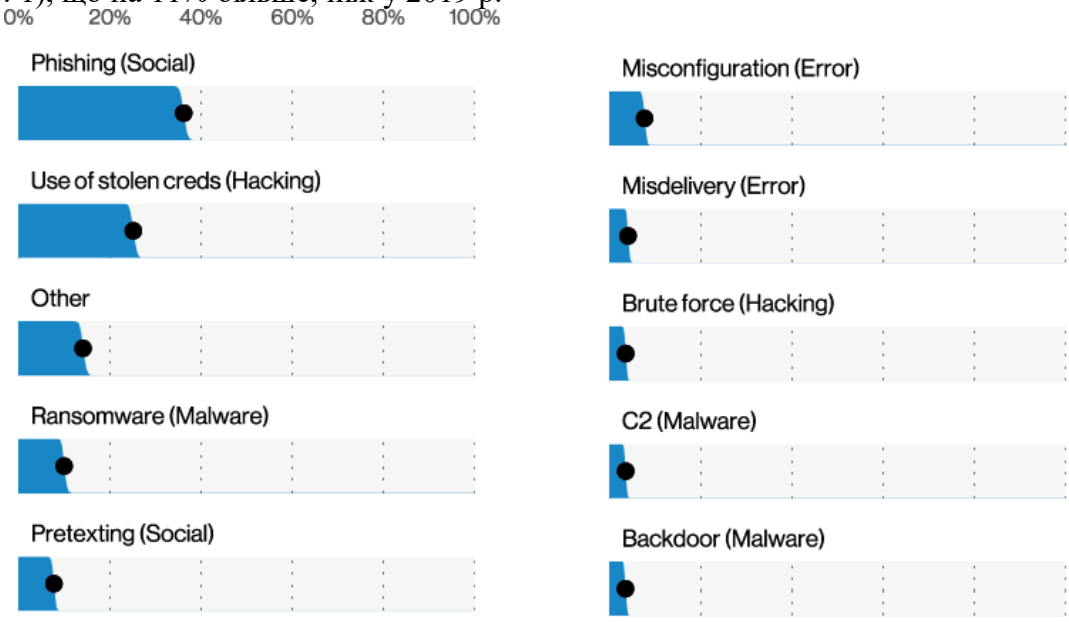

Рис. 1. Рейтинг атак, що стали причиною витоку даних у 2020 р. (фрагмент)

ISSN 2663 - 4023

Такий зріст може свідчити про недостатню обізнаність персоналу компаній та звичайних користувачів з питань кібербезпеки. На даний момент не існує засобів захисту інформації, які могли б точно виявляти та попереджати атаки, в основі яких лежить цільовий фішинг. До того ж, коли зловмисники «експлуатують» людський фактор, впровадження лише програмних та технічних засобів захисту не є достатнім, необхідно також проводити роботи з персоналом – підвищення його обізнаності та періодичне тестування.

Отже, необхідно виділити основні ознаки фішингу та розглянути організаційні методи підвищення стійкості корпоративного середовища до фішингових атак.

Аналіз останніх досліджень і публікацій. До наукових розвідок, присвячених проблемам фішингу та захисту від нього, можна віднести публікації авторів: С. І. Журин, Д. Є. Комарков [2], К. Чепанова [3], Akarshita Shankar [4], Devin Partida [5], Amer Owaida [6], Ryan Naraine [7].

Мета статті. Метою статті є аналіз ознак і методів фішингу з використанням електронної пошти, а також способів захисту від витоку даних або впровадження шкідливого програмного забезпечення в корпоративне середовище внаслідок застосування методів соціальної інженерії відносно персоналу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В більшості випадків фішингові атаки не націлені на конкретного користувача, адже для проведення цільової атаки зловмиснику необхідно витратити більше часу, наприклад, щоб зібрати інформацію про жертву для того, щоб збільшити шанс вдалої фішингової атаки. Класичний же фішинг має таку особливість, як масова розсилка електронних листів з однаковим вмістом. Вони не націлені на якусь конкретну жертву й основна мета зловмисників при такому сценарії атаки – зібрати якомога більше облікових даних та іншої інформації й отримати найбільшу вигоду.

Однак цільовий фішинг, який відрізняється спрямованим характером, хоч і потребує більше часу та зусиль, все одно є доволі популярним серед соціальних інженерів. Такий різновид фішингу є набагато небезпечнішим за класичний фішинг. Хоч він і націлений на конкретну жертву, збитки від нього можуть бути величезними, оскільки зловмисники спеціально збирають якомога більше інформації про жертву, яку вони потім використовують для написання більш переконливого листа. Така інформація може включати імена колег жертви, їх посади та сфери відповідальності, електронні адреси та іншу супровідну інформацію.

До того ж, цільові атаки можуть бути націлені на працівників компанії, які відповідають за критичні процеси або ж за фінансові операції. Так, наприклад, зібравши інформацію про компанію, зловмисники можуть провести фішингову атаку, націлену на співробітника, в обов’язки якого входить проведення авторизації платежів. Як один із сценаріїв, жертва отримує листа нібито від високопосадовця компанії, в якому їй доручено провести крупний платіж на ім’я, наприклад, постачальника компанії. Якщо перейти за посиланням, прикріпленим у листі, воно приведе не до платіжної системи, а на веб-сайт зловмисника.

Як правило, внутрішні та зовнішні комунікації компаній у великій мірі покладаються на використання різних сервісів електронної пошти. Тож не дивно, що у більшості випадків зловмисники, які проводять атаки на корпоративні інформаційні системи за допомогою методів соціальної інженерії, використовують електронну пошту:

ISSN 2663 - 4023

на поштову адресу жертви надсилається лист, зміст якого повинен спонукати її виконати певні дії, наприклад, перейти за посиланням та ввести свої облікові дані, або ж завантажити файл, прикріплений до листа. Такі вкладення зазвичай замасковані під текстові або виконувані файли, що не викликають підозри, та насправді вони можуть містити шкідливе програмне забезпечення. При відкритті такого файлу користувачем, зловмисник зможе отримувати зібрану шкідливою програмою інформацію, наявну в комп'ютері користувача, або ж навіть проникнути в його систему. Приклад фішингової атаки, проведеної за допомогою електронної пошти. наведено на рис. 2 [8].

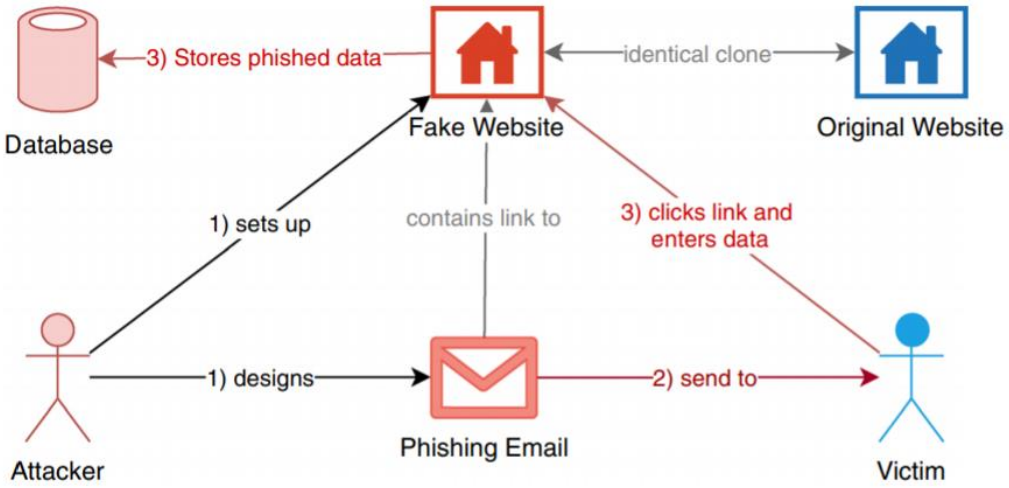

Рис. 2. Приклад фішингової атаки, проведеної за допомогою електронної пошти

Зазвичай в фішингових листах прикріплюється або посилання, яке веде на копію легітимного сайту, підготовлену зловмисником, де він зможе отримати облікові чи персональні дані жертви, або ж файли різного формату, відкриття чи виконання яких призведе до завантаження шкідливого програмного забезпечення або інших негативних наслідків.

Листи з прикріпленими файлами

Дані щодо основних трендів кібератак, які були представлені у звіті Check Point Cyber Attack Trends: 2020 Mid-Year Report [9], показують, що більшу частину вкладень, що прикріплюються до фішингових листів, складають файли формату .exe (26%) та .doc (24%) (рис. 3).

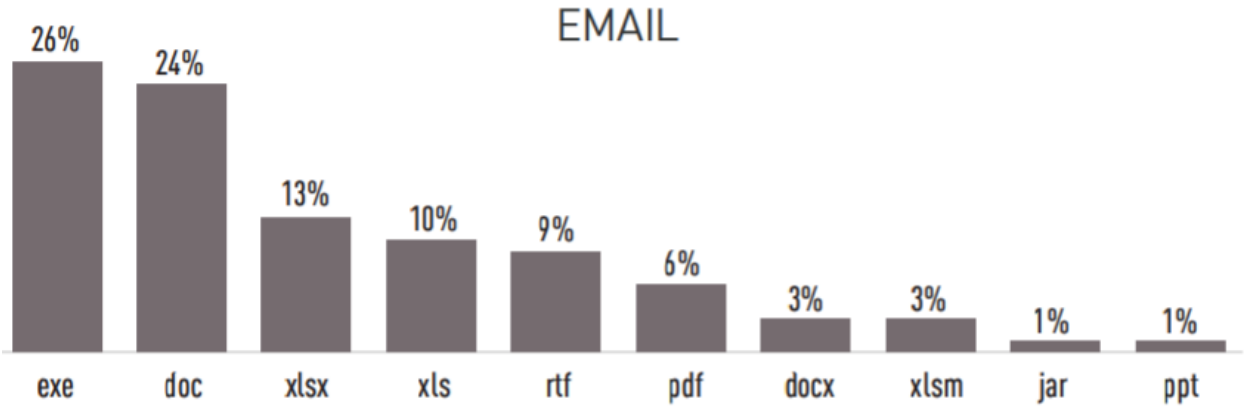

Рис. 3. Розподіл типів шкідливих файлів, що передаються електронною поштою

ISSN 2663 - 4023

До того ж, слід зазначити, що невід'ємною складовою великої кількості кібератак є невиконувані файли [3]. Це офісні документи, які можуть бути прикріплені до електронного листа або які можна завантажити за посиланням. Причина полягає в тому, що виконувані файли формату .exe становлять очевидну потенційну небезпеку, тому більшість поштових сервісів фільтрує листи, якщо до них прикріплені такі файли. Якщо ж розглядати невиконувані файли: текстові документи, таблиці тощо, то у значної кількості користувачів такі файли не викликають підозри, до того ж в більшості випадків листи з прикріпленими невиконуваними файлами не сприймаються, як пряма загроза, і тому пропускаються поштовими сервісами.

Після відкриття файлів формату .doc / .docx, .xls / .xlsx та інших офісних документів жертва навіть може побачити очікуваний вміст файлів, що введе її в оману відсутністю видимих негативних наслідків. Однак такі файли також становлять небезпеку для корпоративних інформаційних систем, оскільки хоч вони і не можуть бути виконані безпосередньо, в програмах, які використовуються для того, щоб їх відкрити, можуть бути наявні вразливості, внаслідок яких зловмисник зможе провести вдалу атаку.

Також зловмисник може використовувати вбудовані засоби офісних додатків, наприклад, функціональність по виконанню макросів – програмних алгоритмів дій, записаних користувачем, які часто застосовуються для автоматизації рутинних операцій: обчислення, форматування тексту, побудови графіків тощо. Однак крім цього макроси можуть використовуватись і для виконання зовнішніх операцій: запуску файлів, запису в реєстр, звернення до Win32 API тощо.

Принцип роботи шкідливих макросів такий: підготовлений зловмисником код записується в DOT-файл, який містить всі глобальні макроси, і замінює собою деякі з них. Після цього всі файли, збережені за допомогою програмної системи, будуть містити макровірус. До того ж, в деяких випадках шкідливий об'єкт не буде розпізнано встановленим антивірусом або системою виявлення вторгнень.

Для того, щоб не стати жертвою атак, реалізованих за допомогою офісних документів, рекомендується:

1. Відключати макроси в офісних додатках. Наприклад, в Word 2016 це можна зробити у розділі Параметри – Центр управління безпекою – Параметри центра управління безпекою – Параметри макросів. Далі необхідно обрати пункт «Відключити всі макроси зі сповіщенням».

2. Використовувати режим захищеного перегляду файлів і попередження виконання даних. Для цього необхідно обрати всі пункти в розділі Параметри – Центр управління безпекою – Параметри центра управління безпекою – Режим захищеного перегляду.

Листи зі шкідливим посиланням

Окрім прикріплених файлів зловмисники можуть відправляти фішингові листи з посиланнями. В такому випадку зловмисник має на меті змусити жертву перейти за цим посиланням на його заздалегідь підготовлений веб-ресурс, де він зможе впровадити шкідливе програмне забезпечення або вкрасти облікові дані користувача, використовуючи вразливості сайту або браузеру жертви.

Для проведення атаки за таким сценарієм зловмисники створюють фішингові сайти, які дублюють дизайн і структуру відомих сайтів. Зазвичай єдиною відмінністю в них є лише доменне ім'я, в іншому вони ідентичні.

Однією з програм, що використовується соціальними інженерами для збору облікових даних, є програма Blackeye [10]. Цей інструмент генерує посилання, яке веде

ISSN 2663 - 4023

на фішинговий сайт – копію сторінок авторизації однієї з 39 соціальних мереж та платформ (рис. 4).

Рис. 4. Стартове меню інструменту Blackeye

Цей інструмент можна завантажити та запустити наступними командами (в терміналі Linux):

```
git clone https://github.com/Git-Ankitraj/blackeye-im.git
cd blackeye-im
chmod +x ./blackeye.sh
./blackeye.sh
```

Після швидкого налаштування можна обрати сайт, копію якого необхідно зробити, та ввести його порядковий номер, після чого Blackeye згенерує посилання, яке необхідно буде надіслати жертві. Як тільки жертва перейде за посиланням на сторінку авторизації, Blackeye вже отримає та збереже дані щодо її IP-адреси, а після введення жертвою облікових даних, перехопить і їх (рис. 5), при цьому жертва при успішній авторизації автоматично перейде на головну сторінку соціальної мережі або платформ, яка була обрана.

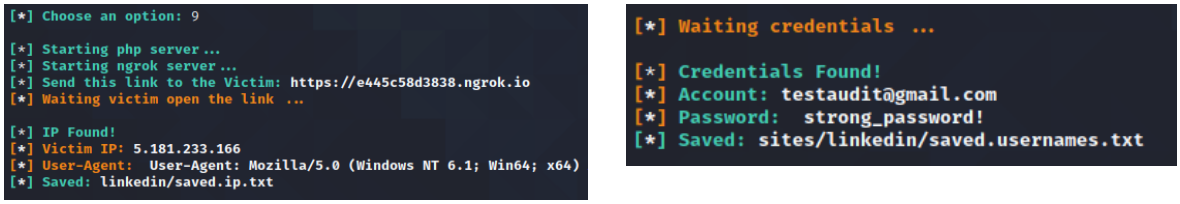

Рис. 5. Робота інструменту Blackeye

Ознаки фішингових листів

Для запобігання витоку даних та впровадження шкідливого програмного забезпечення в корпоративне середовище необхідно періодично проводити навчання та тестування персоналу на предмет розпізнавання фішингових атак. Рекомендується створити інструкцію-пам'ятку для користувачів, слідування правилам якої дозволить зменшити кількість інцидентів, причинами котрих стали фішингові атаки. Зміст пам'ятки повинен охоплювати основні ознаки фішингових листів та для кожної компанії, де це може бути застосовано, містити адресу її корпоративної пошти та доменне ім'я, а

ISSN 2663 - 4023

також приклади, як вони можуть бути змінені порушниками в цілях проведення фішингових атак.

1. Першочергово необхідно звернути увагу на адресу відправника листа. Якщо лист відправлено не з корпоративної пошти, а ім'я відправника відображається як ім'я колеги, високопосадовця, служби технічної підтримки, слід насторожитися.

На щастя, у багатьох компаніях наявні інструменти, які здатні блокувати листи, надіслані з електронних адрес, які не зазначені у переліку допустимих адрес.

2. Також необхідно звернути увагу на адресу отримувача і звернення в листі, якщо вони наявні. Якщо робиться масова розсилка, то, скоріш за все, зловмисник не знає імені жертви і тому в листі не буде вказуватись її ім'я, а замість цього будуть використовуватись безособові звернення типу «Шановний співробітнику!», «Шановний клієнте!» тощо. В полі «Кому» також не буде вказано реальне ім'я жертви.

3. Лист з великою ймовірністю є фішинговим, якщо його написано з помилками в словах, наприклад, «Надішліть пароль» або «Надішліть пороль». Помилки спеціально робляться зловмисниками для обходу спам-фільтрів. Можуть спеціально робитись помилки і в назвах популярних брендів та компаній, наприклад, app1e.com, gooqle.com, raiffaisen.ua тощо.

4. При проведенні масової розсилки для різних регіонів зловмисники можуть перекладати текст листа, тож необхідно звертати увагу на можливі ознаки машинного перекладу, коли конструкція і слова в реченні не пов'язані між собою і не відповідають по змісту.

5. Характерними ознаками для фішингового листа є створення атмосфери невідкладної ситуації, залякування жертви для того, щоб в неї не було часу поміркувати над ситуацією. Так, зловмисники використовують словосполучення виду «термінова перевірка», «останнє попередження», і вимагають, наприклад, негайно пройти авторизацію за посиланням в листі, чи надіслати для перевірки персональні дані, інакше виникнуть якісь негативні наслідки, наприклад, блокування облікового запису. Слід пам'ятати, що відповідальні організації ніколи не попросять своїх клієнтів передавати персональні дані через Інтернет.

6. З іншого боку, в фішингових листах може міститися пропозиція, яка виглядає занадто вигідною, щоб бути правдою. В таких листах може говоритися, що отримувач виграв в лотерею або отримав коштовний приз, а для його отримання необхідно ввести свої персональні дані, номер картки для перевірки, завантажити прикріплений файл тощо.

7. Ще однією ознакою фішингового листа, яка доволі часто слугує причиною крадіжки облікових даних та впровадження шкідливого програмного забезпечення, є підміна домену другого рівня. Оскільки рівні доменів розділяються крапкою, а не слешем, деяких користувачів може ввести в оману підміна такого типу: https://www.mono.bank.ua замість https://www.monobank.ua. Також зловмисник може змінити URL-адресу таким чином, щоб у листі вона здавалася ідентичною до адреси легітимного веб-ресурсу. Для того, щоб побачити справжню URL-адресу посилання, достатньо навести курсор на нього, але не натискати. Після цього в браузері в нижній лівій частині екрану буде висвітлено реальну адресу сайту, на який веде посилання. Якщо вона відрізняється від офіційної адреси банку, компанії тощо, то цей лист фішинговий. Тобто домен другого рівня завжди повинен бути адресою офіційного сайту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Відповідно до вищевказаного аналізу було підкреслено важливість захисту від фішингових атак. Фішингові атаки, що реалізовуються за допомогою електронної пошти – це найбільш розповсюджений різновид фішингу, однак велика кількість користувачів може отримувати фішингові посилання через рекламу в Інтернеті, месенджери чи SMS-повідомлення. Також добре підготовлений соціальний інженер зможе змусити жертву виконати необхідні йому дії в рамках одного телефонного дзвінка.

Оскільки саме працівники компанії є мішенню зловмисників, їм повинні бути надані інструкції щодо розпізнавання фішингових атак та повинно регулярно проводитися їх навчання та тестування. Співробітники повинні бути проінформовані щодо принципів роботи з корпоративними даними та відповідальності, яка на них покладена.

Керівництво компанії повинно розробляти регламент та інструкції щодо зберігання, використання, розповсюдження та передачі інформації третім особам. Співробітники мають бути проінформовані з приводу того, яку інформацію вони мають право передавати і на яких підставах. Якщо третя особа намагається отримати цінну інформацію, співробітники повинні доповідати про цю подію службі безпеки компанії.

Внаслідок збільшення частки фішингу в загальній кількості атак захист від нього залишається доволі актуальним питанням і потребує комплексного поєднання технічних, програмних та особливо організаційних заходів захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *2021 DBIR Master's Guide*. (2021). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

2 Zhurin, S. I., & Komarkov, D. E. (2018). Protection of external information perimeter of organization from spear phishing. *Bezopasnost informacionnyh tehnology*, *25*(4), 96–108. https://doi.org/10.26583/bit.2018.4.09

3 *Как защититься от вредоносных файлов различных типов.* Anti-Malware.ru. https://www.anti-malware.ru/practice/methods/protect-yourself-from-various-malware

4 Shankar, A., Shetty, R., Nath K., B. (2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research*, *14*(9), 2171-2175. https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf

5 *Devin Partida Social engineering cyberattacks and how they're impacting businesses*. (2020). https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

6 *Verizon's 2021 DBIR: Phishing and ransomware threats looming ever larger | WeLiveSecurity*. (2021). WeLiveSecurity. https://www.welivesecurity.com/2021/05/14/verizon-dbir-2021-phishing-ransomware-threats/

7 *Verizon DBIR 2021: Ransomware, Web App and Phishing Attacks Dominate | SecurityWeek.Com*. (2021). Cybersecurity News, Insights and Analysis | SecurityWeek. https://www.securityweek.com/verizon-dbir-2021-ransomware-web-app-and-phishing-attacks-dominate

8 Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, *10*(1). https://doi.org/10.1186/s13673-020-00237-7

9 *Check Point Cyber Attack Trends:* (2020). Mid-Year Report. https://www.antivirus.cz/Blog/Documents/Check-Point-Cyber-Attack-Trends-2020-Mid-Year-Report.pdf

10 10 лучших инструментов для фишинга. https://itsecforu.ru/2020/04/16/10-лучших-инструментов-фишинга/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Yuriy M. Yakymenko
Cand. Military Sc. (Ph.D), Associate Professor, Associate Professor at the
Department of Information and Cyber Security Management
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Dmytro I. Rabchun
Cand. Tech. Sc. (Ph.D), Associate Professor at the
Department of Information and Cyber Security Management
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

Mykhailo M. Zaporozhchenko
assistant at the Department of Information and Cyber Security Management
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

THE PLACE OF SOCIAL ENGINEERING IN THE PROBLEM OF DATA LEAKS AND ORGANIZATIONAL ASPECTS OF CORPORATE ENVIRONMENT PROTECTION AGAINST FISHING E-MAIL ATTACKS

Abstract. As the number and percentage of phishing attacks on company employees and regular users have tended to increase rapidly over the last two years, it is necessary to cover the issue of protection against this type of social engineering attacks. Throughout the pandemic, intruders are finding more and more new ways to cheat, so even experienced Internet users can become a victim to their scams. Due to the fact that e-mail is used in almost all companies, most fishing attacks use e-mail to send malicious messages. The article discusses the main methods used by attackers to conduct phishing attacks using e-mail, signs that the user has become a victim to social engineers, and provides recommendations how to increase the resilience of the corporate environment to such attacks using organizational methods. Because the user is the target of phishing attacks, and the tools built into the browser and email clients in most cases do not provide reliable protection against phishing, it is the user who poses the greatest danger to the company, because he, having become a victim of a fishing attack, can cause significant damage to the company due to his lack of competence and experience. That is why it is necessary to conduct training and periodic testing of personnel to provide resistance to targeted phishing attacks. Company employees should be familiar with the signs of phishing, examples of such attacks, the principles of working with corporate data and their responsibility. The company's management must create and communicate to the staff regulations and instructions that describe storage, processing, dissemination and transfer processes of information to third parties. Employees should also report suspicious emails, messages, calls, or people who have tried to find out valuable information to the company's security service. Raising general awareness through hands-on training will reduce the number of information security incidents caused by phishing attacks.

Keywords: cybersecurity; social engineering; phishing; e-mail.

REFERENCES

1 *2021 DBIR Master's Guide*. (2021). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

2 Zhurin, S. I., & Komarkov, D. E. (2018). Protection of external information perimeter of organization from spear phishing. *Bezopasnost informacionnyh tehnology*, *25*(4), 96–108. https://doi.org/10.26583/bit.2018.4.09

3 *Kak zashchytytsia ot vredonosnыkh failov razlychnыkh typov.* Anti-Malware.ru. https://www.anti-malware.ru/practice/methods/protect-yourself-from-various-malware

4 Shankar, A., Shetty, R., Nath K., B. (2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research*, *14*(9), 2171-2175. https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf

5 *Devin Partida Social engineering cyberattacks and how they're impacting businesses*. (2020). https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

6 *Verizon's 2021 DBIR: Phishing and ransomware threats looming ever larger | WeLiveSecurity*. (2021). WeLiveSecurity. https://www.welivesecurity.com/2021/05/14/verizon-dbir-2021-phishing-ransomware-threats/

7 *Verizon DBIR 2021: Ransomware, Web App and Phishing Attacks Dominate | SecurityWeek.Com*. (2021). Cybersecurity News, Insights and Analysis | SecurityWeek. https://www.securityweek.com/verizon-dbir-2021-ransomware-web-app-and-phishing-attacks-dominate

8 Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, *10*(1). https://doi.org/10.1186/s13673-020-00237-7

9 *Check Point Cyber Attack Trends:* (2020). Mid-Year Report. https://www.antivirus.cz/Blog/Documents/Check-Point-Cyber-Attack-Trends-2020-Mid-Year-Report.pdf

10 10 luchshykh ynstrumentov dlia fyshynha. https://itsecforu.ru/2020/04/16/10-лучших-инструментов-фишинга/