Коцюба Я., магістрант
Науковий керівник: **Сафарова А. Т.,** к.е.н,
доцент кафедри обліку і аудиту
Східноєвропейський національний університет
ім. Лесі Українки, м. Луцьк, Україна

УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДАНИХ У ЗВ'ЯЗКУ З НЕБЕЗПЕКОЮ ФІШИНГОВИХ АТАК

Розвиток та доступність Інтернет-мережі спричиняє зростання злочинної діяльності в режимі онлайн. Спроби отримання стратегічної інформації та особистих даних стають дедалі частішими та є актуальними не тільки для індивідуальних користувачів, а також для керівництва і їх персоналу, що здійснюють економічну діяльність.

Специфічною формою кіберзлочинства є фішинг - атака. На відміну від шкідливого програмного забезпечення, створеного для певних операційних систем, фішингу можуть бути підвладні всі пристрої, у яких наявне підключення до мережі Інтернету.

Фішинг (анг. Phishing (password harvesting fishing) - "ловля в Інтернет - мережі") - це тип автоматизованого глобального шахрайства в Інтернеті, який використовує психологічні методи впливу на користувачів (використовує довіру, знання бренда або викрадення ідентичності) [4].

Фішингові атаки використовують, перш за все, для викрадення даних а саме: адреси електронних скриньок, логіни і паролі для авторизації на особистих аккаунтах, номери банківських карт, пін-коди, терміни дії карт, коди cvv2/cvc2, паспортні дані та ідентифікаційні коди [3].

Вище перелічена інформація в руках шахраїв може бути використана для отримання фінансових переваг, крадіжки інформації, інформаційних боїв або IT-паралічу а саме:

- на серверах електронної пошти (відправлення спаму, підслуховування, економічний шпіонаж, заподіяння шкоди індивідуальним користувачам через викрадення вмісту скриньки);
- за допомогою фіктивних платіжних систем, через отримання даних авторизації доступу або одноразових кодів для переказу: зняття грошей з особистого рахунку в майбутньому використання паспортних даних для отримання кредиту;
- в інтернет-магазинах, що є точною копією відомих світових брендів (використання номерів банківських карт, термінів дії та кодів cvv2/cvc2 для створення електронної копії карти та виплати готівки з неї для власних цілей).

Основними прикладами інтернет- фішингу в 2015-2018 роках являються: розсилка електронних листів з проханням підтвердити логін і пароль; сайти з продажу авіа-квитків, для поповнення мобільного телефону; інтернет-аукціони: товари виставляються на продаж через легальний інтернет-аукціон, однак кошти перераховуються через підроблений веб-вузол; фіктивні благодійні організації, які звертаються з проханням про пожертвування; підпільні інтернет-магазини: товари продаються за вигідними цінами або з великими знижками, що служить розширення

кола клієнтів, та отримання даних банківських карток; інтернет сторінки для переказу грошей через неправдиві платіжні сервіси [2].

На основі дослідження, проведеним Kaspersky Lab у 2018 році частка у секторі глобальних інтернет порталів серед фішингових атак є найбільшою і становить 25,01%, на другій позиції знаходяться банки і фінансові організації – 21,10%, наступними в рейтингу знаходяться IT-компанії – 8,17%, далі інтернет магазини – 8,17%, уряд і податки – 8,17%, E-pay системи – 6,43%, Соціальні мережі та блоги – 3,98%, Інтелектуальні системи виробництва – 2,15%, телекомунікаційні компанії – 1,75% та інше – 8,03%[1].

У період 2015-2018 роках користувачі Бразилії, Китаю, Росії, Грузії, Киргизстану, Казахстану, Венесуели, Португалії, Макао, Республіки Білорусь, Південної Кореї стали предметом фішингових атак.

За даними Інтерактивної карти кібер-загроз створеної Kaspersky Lab у вересні 2018 року Україна займає наступні позиції [1]:

- у рейтингу зараження вірусами займає 23 позицію (30,2%), в топ 5 країн входять: Таджикистан - 45,6%, Киргизстан - 44,7%, Узбекистан – 38,3%, Росія – 37,1 Ємен - 35,8%;
- у рейтингу веб-загроз: Україна займає 9 позицію (22,2%), в топ 5 країн входять: Алжир - 27,9%, Венесуела - 25,5%, Азербайджан -23,3%, Вірменія - 23,1%, Албанія - 23,1%;
- у рейтингу мережевих атак: Україна має низький рівень - 0,8%, в топ 5 країн входять: Каймановські острови - 47,8%, Іран - 18,9%, Гернсі – 15,9%, Пакистан - 11,7% Ізраїль - 10,5%;
- у рейтингу вразливості: Україна - 0,5%, в топ 5 країн входять: Гвінея-Бісау - 2%, Багамські острови - 1,8%, Німеччина - 1,2%, Гуам - 1,2%, Гернсі - 1,1;
- у рейтингу спам: Україна – 0,6%, в топ 5 країн входять: Китай -21,2%, США – 14,8%, Бразилія - 8,3%, В'єтнам - 4,1%, Німеччина - 3,8%.

Отже, для захисту від можливих атак фішингу потрібно виконувати наступні поради від Української міжбанківської Асоціації членів платіжних систем "ЄМА" [2]:

- налаштування кількох електронних адрес (для особистого і офіційного кореспондування);
- ніколи не відповідати на спам та використовувати актуальне антивірусне забезпечення з можливим розширенням анти-спам фільтрів;
- ніхто не повинен володіти паролем або кодом від банківської карти окрім користувача, навіть працівники, які відповідають за їх видання. (Ukr.net). Жоден банк не буде запрошувати такий тип даних через електронний лист;
- не використовувати точку з'єднання громадського Wi-Fi для логування на банківські веб-акаунти, шахраї можуть перехопити ваші особисті дані. Краще скористатися мобільним інтернетом або захищеним з'єднанням;
- користуйтесь тільки відомими та перевіриними платіжними сайтами, які повинні бути зареєстровані на національному домені (наприклад „ .UA")
- перевіряти репутації, віку та терміну реєстрації сайту, особливо інтернет сторінки з поміткою «реклама»; (в адресному рядку браузера потрібно ввести:

whois.com/whois/назва сайту і звернути увагу на дати створення (created) і закінчення терміну (expires);

- звертати увагу на рядок адреси сайту, незначні зміни в процесі користування можуть переадресувати на абсолютно інший неправдивий сайт;
- стежити за встановленням захищеного з'єднання https (в адресному рядку повинен відображатися спеціальний символ – замок, при кліці на замок можна перевірити підтвердження сертифікату для HTTPS).

Якщо користувач підозрює, що опинився жертвою фішингу команда підтримки користувачів support@ukr.net пропонує діяти наступним чином [3]:

- змінити паролі від акаунтів та перевірити на наявність нетипового листування, в разі його наявності – проінформувати отримувачів про неправдиву інформацію;
- при завантаженні підозрілих файлів у розширенні (.exe) – запустити антивірусне сканування ПК;
- негайно заблокувати платіжну картку;
- попередити про небезпеку на інтернет сторінці www. ema.com.ua/report;
- звернутися із інформацією про небезпеку до Кіберполіції онлайн (www.cybercrime.gov.ua).

Список використаних джерел:

1. Карта Кібер-загроз в реальному часі [Електронний ресурс] – Режим доступу до ресурсу: https://cybermap.kaspersky.com/stats/

2. Фішинг в 2017 році: обізнаність - кращий захист від пасток [Електронний ресурс] – Режим доступу до ресурсу: https://ema.com.ua/phishing-statistics-results-2017/

3. Фішинг та мережеве шахрайство [Електронний ресурс] – Режим доступу до ресурсу: http://wiki.ukr.net/Phishing/

4. Що таке фішинг? [Електронний ресурс] – Режим доступу до ресурсу: https://encyclopedia.kaspersky.com/knowledge/what-is-phishing/

Козачук С., студент
Науковий керівник: Сак Т.В., .к.е.н., доцент
кафедри економіки, безпеки та інноваційної
діяльності підприємства
Східноєвропейський національний університет
імені Лесі Українки, м. Луцьк, Україна

СИСТЕМА УПРАВЛІННЯ ФІНАНСОВОЮ СКЛАДОВОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Однією із найважливіших умов забезпечення стійкого зростання підприємства та формування позитивних результатів його фінансової діяльності є існування ефективної системи фінансової безпеки, яка забезпечить захист підприємства від