Кутєпов М.Ю.,
к.ю.н., асистент кафедри кримінології
та кримінально-виконавчого права
Національного юридичного університету
імені Ярослава Мудрого, м. Харків
Данко Н.С.,
студентка 5 курсу, 3 групи,
Господарсько-правового факультету
Національного юридичного університету
імені Ярослава Мудрого

ФІШИНГ В СУЧАСНИХ УМОВАХ

Ключові слова: фішинг, інтернет, шахрайство, інформація
Keywords: phishing, internet, fraud, information

Анотація: У роботі розглянуто один із найпопулярніших та найнебезпечніших видів кібершахрайства в Україні – фішинг. Розкрито причини фішингу та запропоновано заходи запобігання.

Abstract: The paper depicts one of the most popular and the most dangerous types of cybercrime in Ukraine – phishing. The causes of phishing were revealed and measures of prevention were proposed.

На сьогоднішній день все більшої поширеності набирають злочини, що вчиняються у віртуальному світі за допомогою комп'ютерних технологій і різних засобів доступу до віртуального простору. Мова йде про кіберзлочинність. На відміну від традиційних видів злочинів, історія яких налічує століття, таких як вбивство або крадіжка, кіберзлочинність явище відносно " молоде ", а тому боротьба з ним викликає багато проблем у зв'язку з необізнаністю населення в механізмі його здійснення. Це ставить питання запобігання різним проявам кіберзлочинності на перші позиції у дослідженнях та обговореннях.

Найчастіше, коли люди говорять про інтернет, вони не думають про складні взаємодіючі системи. Для них інтернет – просто інформація, яку вони можуть отримати в будь-який час доби. А насправді інтернет – це поле необмежених можливостей, у тому числі і для шахраїв, в арсеналі яких є безліч способів для ведення своєї діяльності, і фішинг як раз таки є одним з них. Фішинг вважають одним із найпопулярніших та найнебезпечніших видів кібершахрайства. Фішинг-атаки – це злочин XXI століття. Саме проблему фішингу ми б і хотіли розглянути у даній роботі.

Спочатку треба розібратися з самим поняттям "фішингу" і що це таке. Фішинг (phishing – похідне від англійського слова fishing (риболовля)) – це відносно новий вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів Мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переведення або обміну валюти, інтернет-магазинів. Шахраї використовують усілякі прийоми, які найчастіше змушують користувачів особисто повідомити конфіденційні дані (наприклад, шляхом надсилання електронних листів із пропозиціями підтвердити реєстрацію аккаунта, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів) [3, с. 229].

Фішинг є одним із найпоширеніших способів шахрайства в Інтернеті, з платіжними картками, спрямований на одержання від жертви конфіденційної інформації про реквізити картки та інші персональні дані. На сьогодні виділяють три види фішингу – поштовий, онлайновий та комбінований. Особливістю досліджуваного виду шахрайства є безпосередня участь особи потерпілого у вчиненні злочинцем правопорушення. Таким чином, наявна "посередницька" діяльність жертви. Вивчаючи типові різновиди її поведінки, особистісні характеристики, можна суттєво зменшити потенційні ризики щодо широких верств населення [2, с. 134-135].

В Україні зафіксована нова форма мобільного фішингу: шахраї спонукають абонентів до "добровільного" переказу грошей зі свого рахунку на особовий рахунок іншого абонента-шахрая.

З вище наведеного матеріалу можна зрозуміти, що жертвами цього злочину стають особи, які мають підвищену віктимність через недостатній інтелектуальний розвиток, недосвідченість у користуванні Мережею Інтернет, довірливість, розсіяність і неуважність. І це зрозуміло, адже професіонали, які розуміються на тому, як забезпечити достатній рівень захисту своїх даних в Мережі, навряд чи стануть жертвами даного виду злочину, хоча така

можливість також не виключається, адже людський фактор припускає вчинення помилок через неуважність.

Фішинг-шахрайства продовжують рости не тільки кількісно, але і якісно з кожним місяцем, на сьогодні таким атакам піддається все більше людей, масова розсилка подібних листів іде на мільйони адрес електронної пошти в усьому світі. Більше того, здійснюється цілеспрямовані атаки на певні групи населення.

Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно іменується "антифішинг".

Фішинговий сайт - це шахрайський веб-ресурс, який виманює реквізити платіжних карток під виглядом надання неіснуючих послуг (поповнення мобільного рахунку, переказів з картки на картку), або веб-ресурс організації, якій користувач довіряє (клон Приват 24), що має на меті збір реквізитів платіжних карток для подальшої крадіжки грошових коштів з рахунків держателів платіжних карток. Більше 90 % фішингових сайтів надають неіснуючі послуги з поповнення мобільного рахунку та переказу коштів з картки на картку [1, с. 170].

Фішинговий сайт дуже схожий на справжній – практично як брат-близнюк. І відмінність його від справжнього сайту може бути всього лише в одній букві, цифрі або символі його адреси в адресному рядку. Бувають іноді і графічні відмінності, але такі невеликі та незначні, що їх практично дуже важко помітити.

Щоб "заманити" потенційних жертв на свій фішинговий сайт, злочинці використовують емоційні важелі. Вони експлуатують страх і необізнаність населення, використовуючи повідомлення про те, що особа могла бути підданою хакерській атаці і перейшовши по заданому посиланню кожен зможе зберегти свої персональні дані. Але в дійсності це лише частина механізму здійснення фішингу, яка надає доступ до інформації про кожного з нас, хто потрапить на "фейковий" сайт. Також досить часто використовують акційні повідомлення. Наприклад, "переведення коштів з картки на картку без комісії", "надішліть ваші персональні дані протягом двох днів і ви отримаєте безлімітний Інтернет ". Все це може слугувати підставою для того, щоб стати жертвою злочину.

За даними веб-аналітиків, у середньому протягом місяця на шахрайський сайт заходить 15-30 тисяч відвідувачів. Слід усвідомити, що число потенційних жертв – величезне, і будь-який користувач інтернету може стати жертвою фішингу.

Деякі злочинці використовують шкідливі вкладення, відкривши які ви створюєте умови, за яких ваш комп'ютер стає "жертвою " злочину. Можна сказати, що злочинець "заражає" ваші технології і комп'ютер стає інфікованим, тобто, піддається розкриттю вашої конфіденційної інформації.

Ми вважаємо, що небезпечність цього злочину полягає в тому, що особа самостійно надає доступ до своїх файлів, своєї інформації. Маючи на меті зареєструватися на певному сайті для отримання послуг, взяти участь у благодійництві чи просто відкрити отримане повідомлення, особа може стати жертвою злочину сама того не усвідомлюючи та не підозрюючи. Дуже складно відрізнити звичайну активність в Мережі від спроб з'ясування конфіденційної інформації. Ця думка підтверджується досить високим рівнем латентності даного виду злочину.

Як в такому разі можна запобігти фішингу? На сьогодні досить поширеним серед видів фішингу є вішинг, що полягає у виманюванні реквізитів банківських карток і переказом коштів на карту злодіїв. Щоб не стати його жертвою необхідно пам'ятати:

- ніколи, нікому і ні за яких обставин не можна повідомляти термін дії платіжної картки і тризначний код безпеки CVV2/CVC2 на зворотному боці картки, а також код підтвердження операції з банківського sms-повідомлення;

- ні співробітники банків, ні представники державних органів та правоохоронці не телефонують громадянам із вимогою назвати термін дії платіжної картки і тризначний код безпеки CVV2/CVC2 на зворотному боці картки, а також одноразовий пароль підтвердження операції, надісланий в банківському sms-повідомленні, або пароль доступу до системи інтернет-банкінгу [1, с. 173].

Фішинг є досить поширеним злочином, про який знає невелика частина населення. Злочинці, використовуючи підвищену віктимність жертв, викрадають конфіденційні дані, що призводить до втрати значних коштів особами, які довірились віртуальному світу. На нашу

думку, щоб запобігти цьому, необхідно розробляти нове програмне обладнання та антивірусні програми, створити системи аутентифікації інтернет-адресів для перевірки відповідності введеної користувачем адреси дійсному серверу та більш широке розповсюдження інформації про відомі види Інтернет-шахрайства користувачам Інтернету. А найголовніше – нам усім треба бути уважними, пильними та обережними, тому що найчастіше люди взагалі не уявляють собі, яким чином їх обвели навкруги пальця.

Список використаних джерел:

1. Нікітська О. В. Методи запобігання фішингу та його різновиди // О. В. Нікітська/ Вісник Академії адвокатури України. - 2017. - Т. 12, N2 1. - с. 169-175.
2. Пивоваров В. В., Терещенко К. В. Шахрайство із банківськими картками: окремі питання віктимологічної профілактики // В. В. Пивоваров, К. В. Терещенко /Карпатський правничий часопис. Серія: Юридичні науки.- 2015.- № 10 .- С. 132-137.
3. Сабадаш В. П. Фішинг як найбільш розвинений вид шахрайства в Інтернеті // В. П. Сабадаш/ Університетські наукові записки. - 2006. - № 2. - С. 228-233.

Міністерство освіти і науки України

**Національний юридичний університет
імені Ярослава Мудрого**

ЗЛОЧИННІСТЬ У ГЛОБАЛІЗОВАНОМУ СВІТІ

Матеріали XVI Всеукраїнської кримінологічної конференції для студентів, аспірантів та молодих вчених

(м. Харків, 12 грудня 2017 р.)

За загальною редакцією
професора *А. П. Гетьмана* і професора *Б. М. Головкіна*

Харків
«Право»
2017

УДК 343.9.01:005.44
ББК 67.61я431
З-68

Злочинність у глобалізованому світі : матеріали XVI Всеукр.
З-68 кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. – Харків : Право, 2017. – 420 с.

ISBN 978-966-937-307-6

ISBN 978-966-937-307-6