режиму для України стосовно відповідальності юридичних осіб: Закон України №314-VII від 23 травня 2013 року. URL: https://zakon.rada.gov.ua/laws/show/314-18#Text (дата звернення: 18.11.2020).

5. Єрмак О. В., Куц В. М. Конфіскація як засіб кримінально-правового реагування: монографія. Чернігів: Видавець Лозовий В. М., 2018. 232 с.

УДК 355.451:004.7

ЖАРОВ ЛЕВ ВОЛОДИМИРОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент,

завідувач кафедри кібербезпеки та DATA-технологій факультету №6

Харківського національного університету внутрішніх справ

ОСНОВНІ ВИДИ КІБЕРШАХРАЙСТВА ТА СПОСОБИ ПРОТИДІЇ

На сьогоднішній день багато людей користуються мережею інтернет та вважають, що вони достатньо освічені в сфері «кібершахрайства». Такі люди помиляються, що для уникнення обману зі сторони досвідчених шахраїв їх знань буде достатньо.

Я зараз перерахую типові схеми якими нікого з вас не здивую:

1) Залякування – шахраї дзвонять жертві та представляючись робітниками державних органів і повідомляють, що хтось із знайомих має деякі неприємності та вимагають хабара [1].

2) Виграш – шахраї повідомляють про деякі виграші, перерахунки пенсій або інших виплат, повернення кредитів. Зазвичай, злочинці називаються працівниками банків, та силових структур [1].

3) Проблеми з карткою – шахрай видає себе за покупця, телефонує продавцю і просить відіслати йому інформацію за картами, бо іншим способом переказати гроші чомусь не виходить. Також шахраї можуть всі реквізити та

іншу інформацію за якою можно отримати доступ до рахунку (СМС від банку, паролі від сервісів, дати та інше) [1].

Навіть знаючи що це з великою вірогідністю шахрайство люди ведуться і скоюють помилки за які потім жаліють. Одним з принципів протидії таким видам злочинів - превенція. Шляхом повторного роз'яснення способів і методів скоєння, запобігання шахрайських дій. Таким чином це зменшить кількість жертв від такого виду злочинів.

Упродовж 2020 року до кіберполіції за формою зворотного зв'язку надійшло більше 41 тисячі звернень громадян, із них понад 80% - щодо шахрайств [2].

«Близько 78% населення України у віці 16 років та старше (приблизно 25 млн осіб) користується інтернетом. З них приблизно 500 тисяч щодня стикаються з кіберзлочинцями. Наймасовішою схемою шахраїв у 2020 став фішинг — відправлення посилань на сайти-підробки. Практично у всіх випадках злочинці використовують методи соціальної інженерії: прикидаються продавцями, покупцями та навіть співробітниками банку, а потім застосовують маніпуляцію, щоб жертва сама віддала свої платіжні дані», — розповів Віктор Нобіуз, керівник відділу бізнес-аналітики компанії OLX Україна [3].

Більш сучасні вид шахрайства:

– Отримання посилки – до вас приходить смс, що для вас прибула посилка, лист і вам потрібно прийти та забрати її, але ви нічого не замовляли. Прийшови на почту вам потрібно сплатити за посилку, лист який в основному коштує до 300грн. Сплативши в ньому ви можете знайти якісь предмет або записку яка не коштує ту суму яку ви потратили за отримання посилки.

– Віруси та інше шкідливе ПЗ – шкідливі програми які потрапляючи на ваш комп'ютер або на телефон ворують всі ваші данні включаючи всі паролі та логіни від усіх сервісів.

– Інтернет-жебрацтво – фейкові сторінки благодійних організацій які прохають про матеріальну допомогу від усіх небайдужих для всіляких добрих цілей, але на справді всі кошти зберігаються у шахраїв.

Отже в інтернеті дуже багато способів для шахрайства і не варто вважати, що ти не потрапиш в халепу від цих шахраїв. Аби убезпечитися від подібних видів шахрайства, кіберполіція радить:

– не передавайте нікому дані своєї банківської картки (особливо CVV-код та пін-код), адже працівники банку ніколи не запитують таку інформацію;

– для безпечного онлайн-шопінгу використовуйте лише перевірені ресурси та обирайте післяплату;

– у разі купівлі на платформі оголошень, обговорюйте деталі угоди тільки в чаті цієї платформи і не переходьте в сторонні месенджери;

– зверніть увагу, що сайти, які приймають онлайн-платежі, мають бути захищеними, для цього в назві адреси вони мають містити https:// та значок «замочок».

– уважно перевіряйте правильність назви необхідного сайту. Один непомітний символ на панелі адреси може означати, що ви потрапили на фішинговий сайт;

– не переходьте за сумнівними посиланнями [2].

Список використаних джерел:

1. Різновиди шахрайства у кіберпросторі. Що потрібно знати для власної кібербезпеки. Частина 1 [Електронний ресурс]. – Режим доступу : https://cybermediatrack.com/kiber-kibershahrajstvo-kiberbezpeka .

2. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті (15 січня 2021 р. 09:54) [Електронний ресурс]. – Режим доступу : https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412 .

3. За рік інтернет-шахраї вкрали 252 мільйони гривень в українців: головні методи злочинців (09 лютого 2021, 15:14) [Електронний ресурс]. – Режим доступу : https://business.rayon.in.ua/news/344808-za-rik-internet-shahrayi-vkrali-252-milioni-griven-v-ukrayintsiv-eksperti-nazvali-golovni-metodi-zlochintsiv .