Обережно, аферисти в інтернеті!

Інтернет-шахраї. Вони використовують будь-які засоби, щоб знайти нову жертву – телефон, електронну пошту чи Інтернет. Завойовують довіру, а коли потрапляєте до них на гачок, просять надіслати гроші. Опісля шахраї зникають.

Олексій розмістив повідомлення про продаж камери на сайті OLX. Одразу ж подзвонив охочий придбати товар. Сказав, сам забрати не зможе, приїде його товариш. Йому й треба віддати камеру.

Олексій Бондаренко – натрапив на аферистів: “Час йшов, нікого не було. І все такі назойливі дзвіночки покупця. Вони почали якось мене дивувати. Він телефонував і казав, “Ну що, товариш під’їхав? Чекайте, будуть кошти, чекайте, скоро кошти я вам надішлю. Товариш от-от має під’їхати.” І як тільки він останній раз сказав, що товариш уже під’їхав, можете вийти і йому камеру віддати. Я сказав: “зачекай, а гроші-то де?”.

Поки Олексій очікував на кошти, аферист весь час дзвонив і покваплював чоловіка, аби той віддав товар.

Олексій Бондаренко – натрапив на аферистів: “Я кажу: “Зачекай, куди ви поспішаєте, я хочу отримати повідомлення від банку, банківської системи про те, що мені зараховані кошти. І ви знаєте, буквально через пару хвилин приходить повідомлення”.

У повідомленні йшлося про те, що на картку Олексія перераховано гроші. Та помилки у тексті смс і невідомий номер відправника виказали аферистів.

Олексій Бондаренко – натрапив на аферистів: “Я зрозумів, що це була маніпуляція свідомістю. Авось, як кажуть поведеться, авось і швидко, і плюс дезорієнтувати людину, з якогось невідомого номеру надіслати повідомлення. Якщо людина

неуважна, поспішає, нервує, то вона дійсно могла би повестися”.

Психолог пояснює: зазвичай, шахраї покваплюють у прийнятті рішення. А якщо запропонувати ще й свої шляхи вирішення проблеми, людина імовірно скористається одним із них.

Ірина Савельєва – психолог: “Коли їй [людині] кажуть: “Треба приймати рішення швидко”, вона буде реагувати [за] запропонованим сценарієм. Тобто, зателефонувати, те, що вони пишуть, “зателефонуйте терміново, наберіть такий код, під’їдьте туди, зробіть те-то”. Тобто оце така буде реакція саме на слово “швидко”.

В Україні на першому місці з 2014 року лишається шахрайство з використанням методів соціальної інженерії. За 2018 рік злочинці найчастіше використовували цей метод під час здійснення незаконних дій з платіжними картками або їхніми реквізитами. Йдеться про введення в оману, щоб громадяни розголосили персональні дані, реквізити платіжних карток, коди/паролі чи здійснили переказ коштів під психологічним впливом на користь шахраїв.

За даними Нацбанку України, найбільша кількість незаконних дій з платіжними картками у 2018 році відбувалась у мережі Інтернет. Це більше половини всіх випадків.

Зокрема, почастішали крадіжки грошей з банківських карток шляхом злому мобільного номера телефону. Аферисти вписують SIM-ку, на електронну пошту приходить повідомлення про зміну пароля в онлайн-банкінгу, а потім і листи про оформлення швидких кредитів.

Олеся Данильченко – заступниця директора Української міжбанківської Асоціації членів платіжних систем “ЄМА”: “Вони отримують доступи до інтернет-банкінгу, банківського інтерфейсу, там вони можуть змінювати якісь ліміти на рахунках, отримувати кредити, грошові, підвищувати кредитні лінії. Тобто безліч опцій. Якщо ви отримували кредит онлайн,

вони можуть отримувати доступ до вашого кабінету на ресурсі у сервісі акредитування і так само змінити ліміт або отримати ліміт, або ще якісь додаткові кредити. Фактично, за вашими даними, але то не ви".

Убезпечити себе від кіберзлочинців можна. Якщо перейти на контрактне обслуговування мобільного оператора – замінити дистанційно сім-карту у мобільному буде неможливо. Тож у такому разі із паспортом громадянина слід звернутися до відділення мобільного оператора і засвідчити свою особу.

Олеся Данильченко – заступниця директора Української міжбанківської Асоціації членів платіжних систем "ЄМА": "Друга є опція. Якщо ви все ж таки ще не наважилися стати контрактним абонентом, хочете щоб у вас був припейд – наперед передплачені послуги, ви можете просто пройти ідентифікацію мобільного оператора. Це треба звернутися до колцентру".

Активізувалися й кіберзлочинці, які намагаються викрасти кошти клієнтів українських банків. Пов'язана нова махінація зловмисників з переходом рахунків на систему IBAN.

З 5 серпня в Україні розпочалося введення міжнародного номера банківського рахунку International Bank Account Number. Про це повідомила пресслужба Національного банку України:

"З 5 серпня 2019 року нові рахунки клієнтам банки відкриватимуть відповідно до вимог стандарту IBAN. У той же час чинні номери рахунків банки будуть міняти відповідно до вимог цього стандарту зі збереженням діючого номера аналітичного обліку".

Шахраї розсилають смс-повідомлення: "У зв'язку із запровадженням IBAN вашу картку заблоковано".

Олеся Данильченко – заступниця директора Української міжбанківської Асоціації членів платіжних систем "ЄМА": "Вони надсилають смс-повідомлення, і вже той, хто отримав смс-повідомлення, телефонує за тим номером, який вказаний начебто

як телефон банку. Тобто це вже говорить шахраю про те, що в принципі людина вже “тепленька”, далі можна з нею вже працювати. Бо якщо [клієнт на це] не відреагував, зрозуміло вже, що нема сенсу [далі його] обробляти, а якщо відреагував, значить, переживає, то можна його далі обробляти, трішечки перевірити ще додаткову інформацію, більше в нього чогось випитати. Ну і фактично вже розвести його за схемою фішингу, коли отримують усі дані, дані про держателя, дані про картку, й потім шахрайські операції проводять в інтернеті”.

Здавалось б, види шахрайств і методи злочинців усі чули та добре знають, але тих, хто піддався на маніпуляції, не меншає.

Ірина Савельєва — психолог: “Яка б людина не була розумна, інстинкт ніхто не відміняв. Тобто ми інстинктивно робимо якісь рухи, а потім думаємо, так треба було робити чи ні. І це завжди така площадка для шахраїв. Насправді на сьогоднішній день дуже багато відео в інтернеті ми можемо подивитися — які є способи, як це роблять вони, які питання задають чи які речення вони говорять. Тобто начебто ми підготовлені, начебто ми про це все знаємо, але коли це стосується саме тебе, коли тобі приходить ця смс чи коли тобі телефонують і кажуть, “так-то і так-то, з вашого рахунку списали всі кошти, вам терміново треба це зробити”, ми будемо включатися.

Та в боротьбі з картковими шахраями тимчасова перевага нині на боці банків та їхніх клієнтів. Головною зброєю боротьби з картковими злодіями банкіри вважають ліквідацію безграмотності користувачів банківських карт і мобільних додатків.

Яна Ємченко, Олександр Кашевко, Дмитро Перов, Київ, “Вісті надії”