Ошибки жертвы

Специалист по кибербезопасности ярославского отделения Банка России Андрей Коценко разобрал типичные ошибки, которые совершают жертвы мошенничества.

Женщине позвонил мужчина, который представился сотрудником службы безопасности банка. Под предлогом предотвращения несанкционированного списания денег, злоумышленник убедил заявительницу перевести накопления со своей банковской карты на указанные им счета. Заявительница лишилась 700 тыс. рублей.

Ошибка: Жертва выполнила все указания звонившего.

Рекомендации: Если вам звонят из банка, финансовой организации или госоргана, уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и перезвоните по официальному телефону организации или на горячую линию банка. Номер нужно набрать вручную.

Ярославна разместила на сайте бесплатных объявлений информацию о продаже детской коляски. Женщине позвонила «покупательница» и под предлогом оплаты товара убедила передать ей реквизиты банковской карты и СМС-коды. В результате со счета были списаны более 180 тыс. рублей.

Ошибка: Сообщила мошеннику конфиденциальные сведения с банковской карты и секретный код из СМС-сообщения от банка.

Рекомендации: Никому не называйте конфиденциальные данные банковской карты. Для осуществления перевода покупателю достаточно знать номер сотового телефона, к которому привязана карта, либо номер карты.

Женщине на мобильный телефон позвонила неизвестная девушка, представилась сотрудником компании, которая предлагает дистанционную работу в Интернете. Убедила установить на мобильный телефон приложение, предоставить реквизиты банковской карты, после чего произошло списание более 15 тыс. рублей.

Ошибка: Скачивание и установка стороннего программного обеспечения по указанию третьих лиц. Сообщила мошеннику конфиденциальные сведения с банковской карты.

Рекомендации: Не размещайте избыточную информацию о себе в соцсетях. Нельзя устанавливать программное обеспечение из сомнительных источников по указанию третьих лиц. На все свои гаджеты нужно установить антивирус. Обязательно ставьте на них пароль!

Не прячьте ваши денежки...

2020 год оказался очень необычным во всех отношениях. В том числе и в сфере преступности. Общее количество преступлений снижается, но растет преступность в сфере онлайн и прежде всего – мошенничества. Об этом на совместной пресс-конференции на прошлой неделе рассказали представители УМВД по Ярославской области и Ярославского отделения Банка России.

■ Ольга СКРОБИНА

Во всем виноват коронавирус

– Традиционная преступность уходит на второй план. Вперед выходят киберпреступления, – с такой констатации начал заместитель начальника УМВД России по Ярославской области, начальник Следственного управления полковник юстиции Дмитрий Жигарев. – Немало этому способствовал период вынужденной самоизоляции, вызванный пандемией коронавируса. Люди в этом году стали больше проводить времени дома. К этим условиям быстро адаптировались и преступники.

Старые добрые способы мошенничества в сфере финансов отходят на второй план. Создавать финансовые пирамиды уже немодно. Жизнь вся уходит в виртуальное пространство, туда же спешат и мошенники. Это подтверждают и цифры статистики. Если в первом полугодии 2019 года в Ярославской области было совершено 931 преступление подобного типа, то в первом полугодии 2020-го – 1622.

Казалось бы, цифры ну очень неприятные. Однако на фоне крупных городов в Ярославской области кибермошенники еще спокойные. В столице, например, три четверти зарегистрированных преступлений связаны с отъемом денег с карт.

У Ярославского отделения Банка России своя статистика по данным преступлениям. За первое полугодие зафиксирован трехкратный рост числа мошеннических звонков. В 2020 году в стране было совершено 16,5 тысячи мошеннических операций на сумму 1,5 миллиарда рублей.

Как ни странно, но изменилась и целевая аудитория мошенников. С традиционных пенсионеров преступники переориентировались на категорию от 30 до 45 лет. Это считается и самая платежеспособная категория, и категория, отлично ориентирующаяся в гаджетах и новых технологиях. Как выяснилось, и обмануть ее несложно.

Служба безопасности банка

Остап Бендер знал 400 честных способов отъема денег. В арсенале современных мошенников способов только 20. Да и честными их назвать сложно. Но можно их сгруппировать в несколько категорий.

Первая – мошенничество в киберпространстве. Сюда можно отнести многочисленные телефонные звонки о «несанкционированном списании денег». Схема такова: человеку звонят якобы от имени службы безопасности банка и говорят, что только что пытались списать деньги с карты. И надо их защитить. Дальше возможны варианты. В одном случае могут просить установить специальное приложение. В другом – сообщить данные карты. Результат один и тот же – мошенник получает доступ к банковскому приложению на телефоне, а через него – ко всем счетам. Соответственно в считанные секунды деньги переводит на свои счета.

– В принципе несанкционированные списания очень редко, но случаются, – говорит заместитель управляющего Ярославским отделением Банка России Евгений Ефремов. – Но сотрудники банка никогда не будут спрашивать данные карты – ее номер, срок действия и прочую конфиденциальную информацию. Если звонящий начинает уточнять эти сведения, значит, это мошенничество. Я рекомендую поблагодарить за то, что предотвратили списание, и повесить трубку. Затем перезвонить в банк по номеру телефона, указанному на самой банковской карте или в договоре. И ни в коем случае не перезванивать на тот номер, с которого звонили.

Под эту же категорию мошеннических звонков можно подвести и случаи, когда человек давал объявление о продаже на сайте бесплатных объявлений. Например, не так давно по Ярославской области прокатилась волна звонков от якобы покупателей собачек и кошечек. Разместившему такое объявление перезванивает якобы покупатель, желающий приобрести товар, но интересуется данными банковской карты; тут же начинают приходить коды доступа, звонящий просит их назвать. Результат все тот же – мошенник получает доступ к личному кабинету в онлайн-банке и уводит деньги со счетов.

Фишинговые сайты

Мошеннические сайты, маскирующиеся под добропорядочные сервисы, существуют давно. Но в этом году они расцвели как никогда. И этому способствовал опять же... коронавирус. Только с начала 2020 года выявлено 119 тысяч таких сайтов! Можно представить объем представительства мошенников в Интернете в этом году.

Из-за коронавируса в этом году были предприняты меры социальной защиты, например, выплаты на детей. Уже через несколько часов после того, как объявили о выплатах, в Интернете появилось множество сайтов, якобы государственных, где надо зарегистрироваться, ввести данные карты, куда должны поступить деньги. Но результат оказывался обратным – деньги не приходили, а тут же исчезали.

Это только частный случай. Но фишинговых сайтов огромное множество, маскируются они под сервисы продажи различных билетов, турпутевок, кэшбэков и многого другого. Где-то предлагают товар со значительной скидкой, где-то социальные выплаты.

Способ не стать жертвой таких сайтов только один – четко знать, что вам положено по закону, и не гнаться за легкой наживой.

Делаем ставки, господа

Третья категория кибермошенничества – это различного рода форекс-площадки. То есть сайты, где предлагается поиграть на курсе валют. Их количество в 2020 году увеличилось в 1,6 раза. При этом легально действующих подобных площадок – считанные единицы. Мошенники соблазняют доверчивых граждан рассказами о том, что можно мгновенно разбогатеть. За дополнительную плату обучают, как действовать на форекс-площадке. Естественно, мгновенного обогащения не получается. Средняя сумма потерь на форексе – от 40 до 100 тысяч рублей.

Страх и алчность

Не надо думать, что стать жертвой мошенников – это удел отдельных беспечных граждан. Жертвами мошенников становились и вполне успешные граждане, которые должны бы по долгу службы быть начеку. Это и учителя информатики, и банковские служащие, и сотрудники полиции.

– Первое, что делают мошенники, – это вгоняют свою потенциальную жертву в состояние стресса, – говорит Евгений Ефремов. – В таком состоянии у человека снижается критическое мышление. Далее преступники начинают играть на двух чувствах – алчности и страхе.

На чувство быстрой наживы работают сообщения о том, что предусмотрены льготы, выплаты, компенсации и надо быстро сообщить данные карты. Или что готовы купить товар, выставленный на сайте бесплатных объявлений, прямо сейчас, но опять же нужны данные карты.

Мотивацию страха задействуют в тех случаях, когда пугают несанкционированным списанием денег.

Но в любом случае общее одно – надо очень быстро принять решение и практически нет возможности перезвонить в банк и проверить информацию.

Как объяснил Дмитрий Жигарев, с раскрытием подобных преступлений есть две объективные сложности. Первая – доказательная база. Ведь мошенники чаще всего звонят с телефонов, приобретенных на посторонних людей и с «левых» сим-карт. После того как достигнут своей цели, телефон и симку выкидывают. И уже очень сложно доказать, что звонок совершал именно этот преступник, а не кто-то другой. Вторая сложность в том, что деньги уходят со счетов мгновенно, а на их поиск требуется долгая процедура, осложненная различными формальностями и бюрократическими проволочками. И все это дает кибермошенникам фору в действиях.

...Мы живем в такое время, когда технологии делают жизнь комфортной. Но чем удобнее нам, тем удобнее и преступникам. И это надо помнить. А еще надо помнить, что мир становится прозрачнее, мы сами в соцсетях выкладываем все подноготную о себе. Почему этой информацией не должны пользоваться преступники в охоте за нашими деньгами? Да, полиция и банки должны противодействовать кибермошенникам. Но сделать так, чтобы не стать их жертвами, – целиком наша ответственность. ■