Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. Однако технологии порождают и новые виды преступной деятельности.

Владельцы банковских карт, чтобы не стать жертвой киберпреступлений, нуждаются в постоянном повышении уровня своей цифровой грамотности.

Поговорим об основных видах киберпреступлений, связанных с хищением денежных средств:

мошенничество, совершаемое через социальные сети;

«фишинг»;

«вишинг».

МОШЕННИЧЕСТВО ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ

Мошенничество в социальных сетях – очень частое явление, причем, существуют разнообразные его виды.

Как обманывают:

Получив несанкционированный доступ к аккаунту пользователя (методом подбора пароля, с использованием поддельных «фишинговых сайтов», вредоносного программного обеспечения), злоумышленник осуществляет рассылку друзьям сообщений мошеннического характера. Далее злоумышленник ждет отклика от ничего не подозревающих интернет-друзей, а получив его, убеждает под разными предлогами передать денежные средства или конфиденциальную информацию.

Некоторые примеры таких сообщений приведены ниже:

«Машенька, я нахожусь в России, у меня украли кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (либо на мобильный номер телефона, кошелёк в электронных платежных системах QIWI, WebMoney или номер банковской платежной карты и т.д.) 5000 рублей (мошенник имеет ввиду российских, т.к. не знает, что в Беларуси указанная сумма столь существенна). Все верну по приезду.»;

«Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом отдашь мне. В долгу не останусь!»

Чтобы убедиться, что это действительно ваш знакомый, необходимо ему позвонить или во время переписки задать вопрос, на который мошенник гарантировано не будет знать верный ответ. После этого уже можно точно знать, кто именно просит деньги.

ФИШИНГ

«Фишинг» – один из методов мошенничества, который заключается

в том, чтобы подделать страницу платежной системы и получить данные банковской карты владельца. Фишинговый сайт – это сайт или страница сайта точно копирующий настоящий. Чаще всего подделывают платежные системы и почтовые сервисы (Белпочта, Европочта, СДЭК). Поддельные страницы часто присылают в мессенджерах продавцам товаров с сайтов объявлений якобы для получения предоплаты за товар и оформления доставки. В данном случае фишинговые страницы содержат сведения о продаваемом товаре и абсолютно повторяют фирменный стиль и сервисы (такие как онлайн-консультант) того сайта, который копируют. Назначением является получение от продавца путем введения в ячейки всех данных банковской карты, включая полный номер и трехзначный код с обратной стороны карты. Эти конфиденциальные данные, которые заполучает создатель страницы, дают возможность перевести все деньги с карты владельца. Отличием фишингового сайта является то, что ссылка на него направляется лично в мессенджере, а интернет-адрес в названии похож на настоящий, но имеет незаметное отличие в одной букве или цифре. Примеры фишинговых страниц: belpochta.by, bellpost.by, belpocht.by, belpost.be, europocha.be, kufar.cc, bel-bank.online.by и подобные.

ВИШИНГ

«Вишинг» – один из методов мошенничества, который заключается в том, что злоумышленники, подменяя реальный номер телефона на номер телефона банка, и выдавая себя за сотрудника банка или правоохранительных органов под предлогом отмены операции (отмены онлайн-кредита, возврата случайно списанной суммы или разоблачения недобросовестного сотрудника банка) выманивают у держателей платежных карт конфиденциальную информацию – номер, срок действия, трехзначный код на обороте – или побуждают к установке программного обеспечения (удаленного доступа) для действий с интернет- или м-банкингом.

К примеру: случай произошел в Новополоцке. Местная жительница в ходе телефонной беседы с якобы сотрудником банка передала ему секретные сведения о реквизитах карты, своем идентификационном номере паспорта и коды из смс-сообщений от банка для подтверждения операций. В итоге женщина лишилась более 30 тысяч долларов.

Или еще один: после телефонного общения с якобы сотрудником банка женщина потеряла более 20 тысяч долларов. Мужчина, используя мессенджер Viber, в ходе разговора представился сотрудником банка и указал, что прямо сейчас с ее карт-счета осуществляется попытка списания денежных средств и для отмены

несанкционированной операции необходимо установить на мобильное устройство или компьютер дополнительное программное обеспечение, а также передать коды из смс-сообщений от банка. Установленная женщиной программа предоставила мошеннику удаленный доступ к компьютеру, где с помощью кодов из смс он вошел в интернет-банкинг и перевел все деньги на свой счет.

Также, мошенники могут перечислить небольшую сумму денег на вашу карту и позже попросить вернуть деньги на указанные реквизиты. Целью такого обмана является пополнение именно вами какого-то определенного счета, например, как подтверждение готовности оплаты вами за дорогостоящие вещи, взятые мошенником в кредит. В таком случае необходимо обратиться в банк с заявлением о незаконно зачисленной сумме.

Еще одним из предлогов для совершения преступления может быть сообщение о том, что недобросовестный сотрудник банка разгласил ваши личные данные, вследствие чего несколько банков одновременно оформили заявки на открытие кредитной линии. Для аннулирования этих кредитов необходимо обратиться в банки с заявлением на кредит, а полученные деньги нужно будет перевести на указанный специально созданный счет (злоумышленнику) для закрытия случайно оформленного кредита, чтобы не портить кредитную историю.

Такое преступление случилось в начале 2021 года. Молодая девушка из Витебска, мама двоих детей, после разговора с сотрудницей банка оформила на себя кредиты на потребительские нужды в трех банках города почти на 16 тысяч рублей, а полученные средства перевела мошенникам.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ КИБЕРПРЕСТУПНИКОВ

Никому ни под каким предлогом не передавать номер банковской платежной карты, срок действия, трёхзначный секретный код на обороте, логины и пароли доступа к банкингу, коды для подтверждения операций из смс-сообщений от банка.

Использовать услугу «3D Secure» и лимиты на максимальные суммы онлайн-операций (нужно подключить в настройках банкинга или в банке).

Для онлайн-покупок оформить отдельную карту (в том числе виртуальную) и не держать на ней большие суммы.

Быть осмотрительными, совершая покупки в Интернете – использовать только проверенные и официальные сайты, внимательно проверять адрес сайта.

Больше информации в Телеграм-канале «Цифровая грамотность» (@cifrgam).