КАК ЗАЩИТИТЬ СЕБЯ ОТ ИНТЕРНЕТ-МОШЕННИЧЕСТВА!

Мошенники постоянно совершенствуют схемы обмана, чтобы заполучить ваши деньги. Для связи кроме интернет-звонков в мессенджерах, таких как Viber, Telegram или WhatsApp, могут использовать стационарную телефонную и мобильную связь, а также интернет-видеосвязь. Чаще всего они представляются сотрудниками правоохранительных органов, работниками операторов сотовой связи, государственных или банковских организаций, реже – вашим родственником или руководителем, брокером или трейдером криптобиржи.

НАИБОЛЕЕ АКТУАЛЬНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

❖ Сообщают о возникшей проблеме и, войдя в доверие, предлагают помощь в ее решении. Например, жертву ошарашивают подозрением в соучастии в **преступлении, следовательно, вероятностью проведения обыска и изъятием денежных средств**. Для их сохранения предлагают перевести наличные на якобы защищенный счет или передать якобы работнику банка **для декларирования.**

❖ Сообщают, что **закончился срок действия договора на услуги связи** и убеждают по ссылке из мессенджера скачать фейковое приложение, чтобы продлить услугу. Такие приложения дают возможность мошенникам видеть всю информацию с экрана смартфона (коды из смс, логины и пароли к банкингу). Надо знать, что безопасно скачивать приложения только из официальных магазинов «Google Play», «App Store», «App Gallery», а не по направленным ссылкам.

❖ Интернет-преступники умело пользуются возможностями нейросетей. При получении образца голоса или фото они создают фейковые сообщения или видео **от имени родственников или знакомых**. Позже контактам жертвы рассылают такие поддельные **просьбы о материальной помощи на лечение на банковскую карту или через «знакомого».**

❖ Самые опасные кибермошенники те, которые **представляются брокерами или трейдерами торговых площадок и предлагают жертве увеличить доход, инвестировав небольшую сумму**. В Интернете они размещают сайт несуществующей биржи с графиками и диаграммами. Регистрируют вкладчикам личный кабинет и демонстрируют якобы полученный доход. Иногда дают вывести небольшую часть денег, но всегда убеждают продолжать вкладывать бóльшие суммы, которые, например, одолжить у знакомых, получить в кредит или от продажи жилья.

❖ Для вывода похищенных денег мошенники всегда используют подставных лиц – дропов, которые за вознаграждение предоставили доступ к своим банковским счетам. Дропы являются звеньями преступной цепочки и нужны для перевода денег через несколько банков на иностранные счета или в криптовалюту**. Дропы несут ответственность по ст. 222 УК** вплоть до 10 лет лишения свободы.

❖ В нашей республике разрешено покупать и продавать криптовалюту за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) только у криптобирж (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц является незаконным и запрещается. Порядок осуществления сделок с криптовалютой определен Указом Президента Республики Беларусь от 20.09.2024 № 367, за нарушение которого предусмотрена ответственность по ч.3 ст.13.3 КоАП в виде штрафа с конфискацией всей суммы дохода.

❖ **Будьте бдительны! Эти знания помогут вам сберечь ваши деньги!**

На территории Гродненской области наблюдается рост количества фактов совершения специфического вида противоправных деяний в сети Интернет. Такие преступления выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем мошенничества либо использования компьютерной техники. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.

Рассмотрим подробнее алгоритм противоправных действий преступника. Для начала ему необходимо завладеть средством связи с потенциальным потерпевшим, обладающим определенной суммой денежных средств. В современном цифровом обществе в качестве такого средства связи все чаще используются электронные ресурсы, среди которых преступника особо привлекают учетные записи в социальных сетях, электронные почтовые ящики, аккаунты в различных программах, предназначенных для обмена сообщениями. Злоумышленник, используя небрежное отношение владельца сайта к обеспечению сохранности конфиденциальной информации (логинов, паролей) о пользователях либо беспечность самих пользователей, стремится получить реквизиты доступа к чужим учетным записям. При этом такая беспечность со стороны пользователей может проявляться в:

– попадании на удочку «фишинговых» (имитирующих настоящий) сайтов;

– вводе логинов и паролей от своих учетных записей в соцсети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах;

– использовании идентичных реквизитов для авторизации на различных ресурсах;

– использовании слишком легких паролей;

– отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ и др.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы, имеет возможность ознакомиться с ее содержимым, изучить список контактов, с которыми жертва поддерживает отношения. Зачастую преступник осуществляет смену пароля доступа к учетной записи, тем самым блокирует доступ законному владельцу к аккаунту. Далее злоумышленник осуществляет рассылку всем либо избранным контактам владельца взломанной учетной записи сообщения мошеннического характера.

Следует констатировать, что фантазия преступников безгранична, вариантов формулировок таких просьб множество, приведем некоторые примеры таких сообщений:

– «Вася (*к примеру*), я нахожусь в России, у меня украли кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (*здесь может быть мобильный номер телефона, кошелёк в электронных платежных системах Яндекс.Деньги, QIWI, WebMoney или других*) 5 000 (*мошенник имел ввиду российских, знал бы он, что в Беларуси указанная сумма столь существенна, он бы уточнил*) рублей. 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!»;

– «Я помогаю в сборе средств для лечения моей дальней родственницы, у нее серьезная болезнь, нужно много денег. Перечисли, если есть возможность, хоть какую-то сумму на кошелек».

Отметим, что выше описанные действия составляют диспозицию таких статей Уголовного кодекса Республики Беларусь, как:

– 349 «Несанкционированный доступ к компьютерной информации» (в данном случае предусмотрено максимальное наказание до двух лет лишения свободы);

– 350 «Модификация компьютерной информации» (до трех лет лишения свободы);

– 351 «Компьютерный саботаж» (лишение свободы на срок от одного года до пяти лет).

Далее преступнику остается ждать отклика от ничего не подозревающих собеседников и проявлять свои способности в риторике и убеждении.

В случае, когда потерпевший отзывается на уловку преступника и, будучи обманутым, сам осуществляет перевод средств на предложенные реквизиты, в действиях злоумышленника усматривается состав преступления, предусмотренного статьей 209 Уголовного кодекса Республики Беларусь «Мошенничество» (в зависимости от суммы похищенного максимальная ответственность может составлять как три, так и десять лет лишения свободы).

Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение путем использования компьютерной техники» (также в зависимости от суммы максимальное наказание варьируется от 3 до 15 лет лишения свободы, кстати ответственность за совершение указанного преступления наступает с 14-летнего возраста и Законом не предусмотрена минимальная сумма хищения). При этом надеяться на то, что преступник в данной ситуации оставит на Вашем карт-счете хоть какую-то сумму, к сожалению, не приходится.

Обратившись к статистике, можно констатировать: в текущем году на территории Гродненской области возбуждено порядка 50 уголовных дел по фактам несанкционированного доступа к учетным записям пользователей в сети Интернет, блокировки и модификации их содержимого. В результате зафиксировано более 30 случаев хищения денежных средств граждан, при этом наблюдается паритет мошенничеств и хищений путем использования компьютерной техники. Суммы похищенного обычно находятся в пределах от 20 до 200 белорусских рублей, однако имели место и случаи, когда граждане расставались с более существенными суммами, максимальная из которых приблизилась к 1 000 рублей.

В результате анализа полученной технической информации установлено, что в большинстве случаев противоправные деяния осуществлялись с использованием компьютерной техники, находящейся за пределами Республики Беларусь. В настоящее время правоохранительными органами с использованием механизмов оказания международной правовой помощи осуществляются дальнейшие мероприятия, направленные на установление личностей злоумышленников и привлечение их к установленной Законом ответственности.

Необходимо отметить, что совершение транзакций по банковским платежным карточкам самим владельцем либо нарушение правил пользования карточками, выразившееся в передаче платежных реквизитов третьим лицам, практически не оставляет шансов вернуть денежные средства с использованием действующего в Беларуси принципа нулевой ответственности пользователей банковских карточек.

Учитывая изложенные выше факты, приведем некоторые рекомендации для пользователей сети Интернет, которые могут снизить вероятность совершения противоправных деяний:

– для выхода в сеть Интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;

– используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения;

– при использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно вы зашли на поддельную его копию;

– вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);

– не используйте одинаковые логины и пароли на различных сайтах;

– не используйте слишком легкие пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т.д.);

– по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;

– остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;

– с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (даже финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным Интернет-каналам;

– при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь), либо в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;

– если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;

– при осуществлении Интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но в общем случае, можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к окружающим нас явлениям и событиям.

В случае совершения в отношении Вас аналогичных противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства либо обнаружения факта совершения преступления.

Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!