В целях профилактики киберпреступлений
Смолевичский районный отдел Следственного комитета
Республики Беларусь информирует

Способы совершения киберпреступлений

В настоящее время телефонные звонки стали популярным подспорьем для осуществления противоправных действий. Злоумышленники представляются работниками банков или выдуманных организаций. При телефонном разговоре злоумышленники пытаются испугать жертву. Для этого они используют фразы: ***"с Вашей картой происходят мошеннические транзакции", "со счета уже списаны деньги и спасти их можно в считанные минуты", "от Вашего имени направлена заявка на кредит, нужно срочно ее отменить", "на Ваш счет ошибочно зачислен перевод, его нужно вернуть".***

После таких фраз человек начинает волноваться, т.к. под угрозой его сбережения, также свою лепту вносит фактор внезапности, и необходимости быстро принять решение. Далее следуют вопросы о номере карты, ее сроке действия, трехзначном коде на обороте и цифры из SMS-сообщения, после чего все находящиеся на счете деньги переводятся на счет злоумышленников. В большинстве случаев номер телефона злоумышленников имеет принадлежность к зарубежным операторам сотовой связи.

Одним из способов обмана являются сообщения, согласно которым человек стал победителем кого-либо розыгрыша и для получения приза необходимо лишь оплатить его доставку. Однако, после оплаты таких «призов» кроме потерянных денег человек ничего не получает.

«Одноклассники» наиболее уязвимый сайт для злоумышленников, это связано с его аудиторией, доверием которой охотно пользуются мошенники. Для осуществления преступной деятельности мошенники пытаются осуществить «взлом» страницы в социальной сети, для последующей рассылки сообщений или создают страницу, идентичную странице иного пользователя и с ее помощью просят перевода денежных средств, для чего рассылают сообщения с просьбами о переводе денежных средств, представляясь близким родственником или друзьями.

Популярный способ обмана – это использование сайтов объявлений. Для этого используются всем известные интернет-сайты объявлений, которые стали хорошим подспорьем для совершения преступлений. Прослеживаются 2 основных способа обмана граждан. При первом способе, жертвой злоумышленников является продавец каких-либо вещей. Под видом покупателя злоумышленник начинает вести переписку по поводу интересуемого товара. Переписка может продолжаться до недели, после чего злоумышленник соглашается приобрести вещь, для чего просит отправить ее по почте, а он в свою очередь переведет денежные средства на Вашу карту. Для этого злоумышленник высылает ссылку на сайт (схожий на сайт интернет-банкинга), где необходимо указать данные банковской карты, на которую поступят деньги за Ваш товар. После заполнения анкеты на фальшивом сайте, с банковской карты, реквизиты которой были указаны, списываются все имеющиеся денежные средства.

При втором способе жертвой мошенников является покупатель. В такой ситуации имеется размещенное мошенниками объявление о продаже какой-нибудь вещи. При переписке с продавцом, он сообщает, что работает по предоплате, а покупку отправляет по почте или одной из служб доставки. Также он указывает реквизиты банковской карты, на которую необходимо перевести деньги за товар. После оплаты покупки мошенник высылает фотографию чека с почты или квитанции (якобы подтверждающей отправление посылки) однако, товар не приходит, а продавец прекращает выходить на связь.

Алгоритм телефонного обмана

Отмечается рост мошенничеств, совершенных под предлогом оказания помощи родственникам(знакомым), которые якобы стали виновниками дорожно-транспортного происшествия (далее ДТП), и для возмещения ущерба и не привлечения их к ответственности потерпевшему необходимо передать «представителю правоохранительных органов» определенную сумму денег.

Жертвами преступников чаще всего становятся женщины в возрасте от 60 лет и старше.

Согласно официальным сведениям в 2022 году по оконченным уголовным делам установлен материальный ущерб, причиненный гражданам, свыше 180 млн. рублей, более 20% которого приходится на состав преступления - мошенничество. Количество лиц, пострадавших в текущем году от мошеннических действий, увеличилось в два раза (с 4 814 до 9 521).

Алгоритм действий преступников выглядит следующим образом:

1. В открытых источниках сети интернет, как правило, в тематических телеграм-каналах («Праца Рэспублика Беларусь», «Работа подработка заработок», «Работа Гродно», «Работа Брест», «Работа подработка Минск», «Работа Минск», «LOL.STEAM», «Доставка из РП в РБ», «Быстрый заработок», «Быстрый заработок, Беларусь» и т.д.) неустановленными лицами размещаются объявления о работе курьерами. При этом лицо, выразившее желание работать, должно пройти ряд верификационных процедур: предоставить фотокопию паспорта, ответить на видеозвонок и т.д. Курьеры осведомлены о криминальном характере деятельности, за свою работу получают 5-15% от передаваемой суммы в зависимости от ее размера.
2. Курьер получает указание выбыть в населенный пункт (район, микрорайон), жители которого будут получать звонки от преступников.
3. Потерпевшему на стационарный телефон поступает звонок (используются средства IP-телефонии, география шлюзов, обеспечивающих трансляцию IP-сигнала в телефонную сеть, весьма обширна: Армения, Вьетнам, Молдова, Латвия, Литва, Россия, Эстония и т.д.). В ходе общения потерпевшего убеждают в том, что он разговаривает со своим близким родственником.
4. К беседе подключается «представитель правоохранительных органов», как правило, «следователь», который разъясняет необходимость «возмещения вреда», уточняет ФИО и адрес потерпевшего, номер мобильного телефона.

5. Потерпевшему поступает звонок «следователя» на мобильный телефон, при этом он просит не прерывать разговор по стационарной сети. В разговоре потерпевшего убеждают передать деньги «помощнику следователя», «адвокату» и т.д. В половине случаев «следователь» просит написать в трех экземплярах заявление на имя «начальника» Следственного комитета о добровольном возмещении вреда, причиненного ДТП, на проведение операции «пострадавшему» в ДТП и просьбой о не привлечении к уголовной ответственности (с целью предоставления дополнительного времени курьеру, который выбыл на адрес потерпевшего).

6. Курьер получает уточненный адрес, выезжает за деньгами. Все это время, вплоть до получения подтверждения от курьера о получении денег, потерпевший остается на связи с преступниками.

7. Курьер передает деньги «нанимателю» (банковский счет, электронный кошелек, криптокошелек или наличными третьему лицу).

Таким образом, помимо курьеров в преступную группу входят лица, их вербующие и руководящие ими, а также непосредственно операторы, осуществляющие звонки. При этом вербовщик может действовать самостоятельно, а лицо, дающее указания курьеру, находится в непосредственном взаимодействии с оператором в момент разговора.

Курьеры являются наиболее уязвимым местом преступной организации, остальные участники максимально обезличены. После задержания они, как правило, оказывают содействие правоохранительным органам, однако их осведомленность не распространяется дальше имени (никнейма) вербовщика и «куратора» в интернет-мессенджере.

В среднем курьер до его задержания обеспечивает не более 3-4 передач. Организаторы преступной схемы осознают высокую степень вероятности задержания курьеров, их замысел заключается в том, чтобы курьер контактировал с деньгами минимально возможное время. Для обеспечения анонимности и сохранности наличные деньги переводятся в криптовалюту. Поиском лица, оказывающего услуги по конвертации наличных денег в криптовалюту, занимаются непосредственно организаторы преступления.

При раскрытии преступлений указанной категории имеются объективные трудности в установлении организаторов, которые нередко находятся на территории иностранных государств и вовлекают в преступную деятельность граждан Республики Беларусь. Полученные от потерпевших денежные средства переводятся на электронные кошельки и банковские счета.

Чтобы не стать жертвой указанных мошенников при телефонном звонке, необходимо не поддаваться чувству паники и волнению, объективно оценивать получаемую информацию. Прежде чем предпринимать какие-либо действия необходимо связаться с родственниками и сообщить в милицию о произошедшем.

Опасность объявлений в социальной сети «Инстаграм»

Социальные сети уже на протяжении длительного времени используются злоумышленниками для обмана доверчивых граждан, однако наибольшую популярность у мошенников получила социальная сеть

«Инстаграм».

В текущем 2023 г. от обмана путем продажи товаров в данной социальной сети пострадало более 40 жителей г. Смолевичи (Смолевичского района).

Мошенники часто ориентируются на спрос населения, активно предлагая сезонные товары. Например, летом продают инвентарь для сада и дачи, гамаки, кресла-коконы, в новогодние праздники – ели и иные новогодние товары. Вне зависимости от поры года популярностью пользуются комплекты одежды и отдельные ее позиции.

Для завлечения покупателей мошенники зачастую используют следующие уловки:

- цена, заметно сниженная по сравнению с торговыми сетями и официальными сайтами производителей;
- дополнительные скидки за приобретение нескольких товаров либо комплектов;
- бесплатная доставка;
- большое количество исключительно положительных отзывов.

Если Вы решили приобрести какой-либо товар в «Инстаграме», то проверьте аккаунт магазина по следующим признакам:

1. низкая цена на товар;
2. обязательная предоплата;
3. отсутствие самовывоза;
4. отсутствие сведений о продавце, контактной информации, в т.ч. учетного номера плательщика;
5. наличие неточностей и несоответствии в описании товаров;
6. излишняя настойчивость и навязчивость менеджеров;
7. пересылка для подтверждения достоверности сделки фото паспортов, документов.

Любой из этих критериев – серьезный повод задуматься о целесообразности совершения сделки и если под описание интернет-магазина попадают два или более пунктов, то необходимо воздержаться от покупок на данном сайте.

Как же не стать жертвой киберпреступника?

Для этого нужно запомнить и руководствоваться следующими рекомендациями:

- использовать сложные (уникальные) и различные пароли доступа к своим учетным данным (электронным почтовым ящикам, аккаунтам в социальных сетях, личным кабинетам системы «Интернет-банкинг»);
- не переходить по сомнительным (фишинговым) ссылкам.
- использовать специальное программное обеспечение (антивирус, расширение для веб-браузеров), чтобы избежать посещения сомнительных ресурсов;
- подключить и использовать двухфакторную аутентификацию;

- обмениваться сообщениями в социальных сетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагировать на сомнительные просьбы и предложения

- хранить в тайне ПИН-код к банковской платежной карте;

- ни при каких обстоятельствах нельзя сообщать (передавать) реквизиты банковских платежных карт (номер карты, срок действия, данные держателя, трехзначный код на обратной стороне карты -CVV/CVC номер), фотографии карт, свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг» и коды доступа к нему в виде SMS-сообщений, поступающих из банка;

- использовать услугу «3-D Secure», лимиты на количество и максимальные суммы операций, проводимых посредствам сети Интернет;

- для совершения покупок в сети Интернет использовать отдельную банковскую платежную карту;

- при оплате услуг (товаров) вводить данные банковских платежных карт только на проверенных(популярных) сетевых ресурсах.

Смолевичский районный отдел Следственного комитета Республики Беларусь