О современных способах совершения киберпреступлений на территории Чашникского района

Современные технологии развиваются с огромной скоростью, предоставляя злоумышленникам новые инструменты для осуществления своих планов.

Недостаток осведомленности среди населения о возможных угрозах и методах защиты делает значительную часть общества уязвимой.

По статистике женщины чаще становятся потерпевшими, чем мужчины. Абсолютное большинство проживает в городах. Граждане с высшим в равной степени, как и со средним образованием, подвержены обману. В данном случае образование не формирует иммунитет против наивности: наоборот, уверенность в собственной компетентности иногда ведёт к неосторожности. Поэтому актуальность знаний о кибермошенничествах и осведомленность о методах защиты важны как никогда. Каждый, независимо от уровня образования, должен быть готов противостоять мошенникам.

Мошенники регулярно меняют свои схемы обмана, преследуя одну лишь цель – похитить деньги. По-прежнему являются актуальными телефонное мошенничество.

В большинстве случаев мошенники звонят через мессенджеры (Telegram, WhatsApp, Viber), а также могут использовать стационарную телефонную и мобильную связь, представляясь **сотрудниками мобильного оператора**, под предлогом продления договора или срока действия сим-карты или тарифа предлагают установить поддельное приложение. Для этого в том же мессенджере направляют файл.

Если пользователь запустил файл, то установится фейковое приложение, которое дает мошенникам доступ к данным на устройстве: логинам, и паролям, кодам из смс, фото и сообщениям и другой информации, а также оформить онлайн-кредит на пользователя и похитить деньги.

Следует помнить, что все договора, тарифы и сим-карты бессрочны, сотрудники мобильных операторов не звонят абонентам через мессенджеры и не требуют изменить пароли под диктовку. Если Вы получили звонок через любой мессенджер якобы от оператора – прервите разговор и самостоятельно обратитесь в офис Вашего оператора для проверки информации. Никогда не

устанавливайте приложения по ссылкам, полученным через мессенджеры из неизвестных источников.

Распространены мошенничества, связанные со звонками злоумышленников посредством мессенджеров гражданам, где в ходе беседы злоумышленники представляются **работниками банковской сферы,** сотрудниками правоохранительных органов, сотрудниками государственных организаций, предприятий. Особенно часто представляются сотрудниками Энергосбыта и под предлогом замены счетчиков завладевают паспортными данными с целью оформления кредитов.

Мошенники пытаются убедить граждан в том, что на их имя оформляется кредит в одном из банков и с целью сохранения денежных средств, а также разоблачения недобросовестных сотрудников банковской сферы, убеждают перевести свои денежные средства на «защищенный счет», либо оформить кредиты на собственное имя, для последующего перевода денежных средств на счета злоумышленников. Также телефонные мошенники могут представляться **родственниками граждан и от их имени убеждать в том, что по их вине в ДТП** пострадали посторонние лица и для благоприятного решения вопроса и прекращения уголовного дела им необходимы денежные средства.

Граждане, попавшие под влияние данных мошенников с целью оказания содействия правоохранительным органам в разоблачении недобросовестных работников банковской сферы, теряют бдительность, не удостоверившись в том, кто им звонит, вступают в диалог с мошенниками, оформляют кредиты на собственное имя и в последующем, полученные денежные средства переводят на счета злоумышленников. После этого мошенники прекращают общение с потерпевшими.

Так, у пожилой жительницы г. Чашники посредством сети интернет, в ходе разговора в мессенджере «Телеграмм», мошенническим путем, представившись сотрудниками МТС, а затем правоохранительных органов, под предлогом декларирования всех денег и снятия блокировки с банковских карточек завладели денежными средствами в сумме более 28 000 рублей .

Также одним из самых распространенных способов совершения мошенничеств в глобальной сети Интернет является завладение денежными средствами под предлогом получения **предоплаты за продажу товаров на торговых Интернет-площадках** и в группах в социальных сетях, таких как «Инстаграм», «Вконтакте», «Телеграм», «Куфар» и т.д.

Граждане, заинтересовавшиеся объявлениями о продаже товаров по низким ценам, теряют бдительность, вступают в переписку со злоумышленниками, которые представляются продавцами Интернет-магазинов. В ходе переписки, желая получить товар по выгодной цене в кратчайшие сроки, доверчивые граждане, никак не убеждаясь в добропорядочности продавца, переводят на указанные им счета денежные средства. После этого злоумышленники завладевают этими денежными средствами, прекращают общение с покупателем, товар не высылают.

Набирает популярность такой способ совершения мошеннических действий в глобальной сети «Интернет», как завладение денежными средствами **под предлогом купли/продажи криптовалюты, заработка на акционной бирже.** Когда речь идет про инвестиции, общение может длиться месяцами, мошенник становится жертве чуть ли не другом. Как правило мошенники, имея фото или логотип крупной организации, создают фейковое видео о несуществующих биржах.

В псевдоинвестиции чаще верит молодежь, хотя встречаются и довольно возрастные жертвы. К примеру, жительница г.Новолукомля 1943 года рождения, которая не только вложила в сомнительные проекты все свои сбережения, но и продала свою квартиру.

Не стоит забывать, что с целью получения личных данных владельцев и счетов, мошенники создают страницы-клоны банков, сайтов театров, инвестиционных бирж.

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через промежуточные счета, открытые в белорусских банках на подставных лиц, так называемых «дропов». Часто промежуточных счетов бывает более десятка.

В нашей стране открыть банковский счет может гражданин с 14 лет, с разрешения законных представителей, то есть даже несовершеннолетние могут открыть банковские счета. Этим и пользуются преступники. Находясь за границей, злоумышленники

подбирают лиц, которые согласятся открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет в интернет-банкинга, а также предоставить разовый СМС-код.

Напрямую мошенники в интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Например, в Telegram рассылают объявления о поиске курьеров в любом городе со стабильной оплатой труда, или людей для разгрузки товаров, или людей на вакансию «тайный покупатель», или заманивают обещанием высокой и быстрой оплаты.

Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Кроме похищенных киберпреступниками денег по промежуточным счетам также могут проводиться деньги, полученные от незаконного оборота наркотиков. Ответственность за возникновение прошедших по банковским счетам денег несут владельцы таких счетов.

Надо знать, что статьей **222 Уголовного кодекса Республики Беларусь** предусмотрена уголовная ответственность за распространение из корыстных побуждений находящихся в незаконном владении лица реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам, электронным или виртуальным кошелькам.

Имеются факты, когда в преступную деятельность вовлекались несовершеннолетние.

Чтобы не стать очередной жертвой киберпреступников запомните следующие правила:

– при совершении покупок в Сети Интернет производить оплату необходимо только после получения товара и проверки его состояния;

– не стоит забывать, что мошенники могут представляться вымышленными данными, использовать для подтверждения личности фотографии чужих паспортов, чужие аккаунты в соцсетях, чужие абонентские номера. Наилучший способ общения – личная встреча с продавцом, осмотр товара на месте;

– не доверяйте красивому оформлению сайта или страницы Интернет-магазина, комментариям пользователей. На сегодняшний день создать сайт с любой информацией не составляет труда. Отличить добросовестных продавцов от мошенников стало невозможно;

– покупайте товары в проверенных магазинах, либо перед покупкой проверяйте их посредством мониторинга в сети Интернет;

– не попадайтесь на уловки мошенников, обещающих Вам продать товар по низкой цене, какими бы выгодными не были условия сделки.

– сотрудники правоохранительных органов и работники банков не звонят в мессенджерах и не просят оформить кредит или оказать содействие в поимке злоумышленников, а также не предлагают застраховать и обезопасить денежные средства;

– обращайте внимание на абонентские номера, с которых вам звонят в мессенджерах, чаще всего абонентские номера, с которых звонят злоумышленники, принадлежат иностранным государствам, абонентские номера Республики Беларусь начинаются с кода «+375» ;

– не устанавливайте по указанию неизвестных лиц на своем мобильном телефоне никаких приложений;

– не переводите деньги на «защищенный счет»;

– не сообщайте неизвестным лицам свои персональные данные, реквизиты банковских карт, SMS-коды;

– не переходите по ссылкам от неизвестных пользователей;

– при поступлении подобных звонков немедленно прекратите разговор и сообщите о произошедшем в милицию.

Также рекомендуем подписаться на телеграм-канал «**Цифровая грамотность**», где на регулярной основе публикуется актуальная информация о способах совершения киберпреступлений и методах противодействия им.

(Материал предоставлении Чашникским РОВД)