О профилактике киберпреступлений (дополнительная тема)

Глобальная сеть Интернет стала незаменимым средством повседневной связи, обмена информацией, осуществления платежей, и преступники этим пользуются.

Несмотря на принимаемые сотрудниками органов внутренних дел меры по противодействию киберпреступности, даже при незначительном снижении числа киберпреступлений проблема остается актуальной и требующей постоянного внимания.

По-прежнему **недостаток осведомленности** граждан о современных схемах мошенничества является одной из основных причин, по которым мошенники продолжают успешно действовать. Если граждане не в курсе последних тенденций, они становятся более уязвимыми. Мошенники часто используют психологические приемы, чтобы манипулировать людьми и заставить их совершать действия, которые в противном случае они бы не совершали. Мошенники часто нацелены на людей, которые находятся в состоянии стресса, страха, отчаяния. В такие моменты люди менее склонны к рациональному мышлению и более подвержены влиянию мошенников.

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 приводит к серьезным негативным последствиям. Поэтому актуальность знаний о кибермошенничествах и осведомленность о методах защиты важны как никогда. Каждый, независимо от уровня образования, должен быть готов противостоять мошенникам.

Мошенники становятся все более изощренными, преследуя одну лишь цель - похитить деньги. По-прежнему являются актуальными телефонные мошенничества (**вишинг**).

Звонки на абонентские номера городской/мобильной телефонной связи

В большинстве случаев мошенники выдают себя за сотрудников правоохранительных органов, банковской сферы и других

государственных организаций, предприятий. Звонят через мессенджеры (Telegram, WhatsApp, Viber), а также могут использовать стационарную телефонную и мобильную связь, представляясь сотрудниками мобильного оператора (в том числе за работников коммунальных служб РУП «Витебскэнерго», УП «Витебскводоканал», УП «Витебскоблгаз», а также работников РУП «Белтелеком») под предлогом продления договора/замены счетчиков или срока действия сим-карты/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/паролям, кодам из смс, фото и сообщениям, и другой информации, а также оформить онлайн-кредит на пользователя и похитить деньги.

Часто работают в паре: один представляется сотрудником коммунальной службы, другой - правоохранительных органов или банка, убеждая жертву, что ее данные скомпрометированы, и для «спасения» средств или разоблачения недобросовестных сотрудников банковской сферы, необходимо оформить кредит или перевести деньги на «защищенный счет».

Например, в районный отдел внутренних дел обратилась гражданка, которая сообщила, что ей на мобильный телефон поступил звонок посредством мессенджера «Viber». Мужчина представился сотрудником телефонной компании и сказал, что на счет поступили денежные средства в крупном размере рублей, которые потом со счета были переведены куда-то на Украину на финансирование ВСУ. Затем прислал фотоснимок с какими-то переводами. Далее мужчина сказал, что свяжет с капитаном финансовой милиции. Сотрудник из финансовой милиции стал интересоваться кредитной историей, сообщил, что на женщину оформлены кредиты и для того, чтобы аннулировать уже оформленные кредиты, а также изобличить недобросовестных сотрудников банка, необходимо оформить новые и перевести деньги на указанный счет. В действительности женщина обратилась в отделение банка «Беларусбанк», где оформила заявку на получение потребительского кредита на сумму 17500 рублей и перевела денежные средства на безопасный счет, с которого их похитили мошенники.

Граждане, попавшие под влияние 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.

«Фейк-босс»

Следует отметить, что мошенники продолжают использовать схему «фейк-босс». Для совершения преступлений изучают свою жертву, собирают в сети Интернет сведения о ней и ее интересах, окружении и прочем. Имея образец голоса или фото знакомых, могут создавать фейковые текстовые или видеосообщения.

Как правило, жертве пишет или звонит руководитель и сообщает, что в отношении сотрудников или организации проводится проверка. Задача «фейк-босса» заранее обеспечить нужный психологический эффект для последующего контакта с мошенником, который позвонит позднее и представится сотрудником правоохранительных органов.

Например, потерпевшим от такой схемы мошенничества стал житель города Полоцка. В мессенджере Telegram мужчина получил сообщение от якобы руководителя о том, что в организации проводится внеплановая проверка, в ходе которой выявлено, что кто-то из сотрудников продаёт личные данные работников и, что с ним свяжется проверяющий. Через некоторое время с потерпевшим связался «сотрудник КГБ», который сообщил, что с лицевого счета мужчины в другие страны были переведены денежные средства, а также сбросил ссылку Национального банка, чтобы проверить вышеуказанную информацию. Затем позвонила «сотрудница Национального банка», которая сообщила, что на потерпевшего оформлены кредиты во всех банках города Полоцка и, чтобы их погасить и изобличить «недобросовестных» работников банка, которые могут быть причастны к мошенническим схемам, необходимо взять новые кредиты. Всего полочанин перевел мошенникам более 37 тысяч рублей.

В сентябре такие сообщения рассылались от имени председателя райисполкома, но бдительные работники не поддались на провокацию.

ИНВЕСТИЦИИ

Набирает популярность такой способ совершения мошеннических действий в глобальной сети «Интернет», как завладение денежными средствами под предлогом купли/продажи криптовалюты, заработка на аукционной бирже. Часто мошенники, имея фото или логотип крупной организации, создают поддельные сайты и приложения, имитирующие популярные криптовалютные платформы, фейковое видео о несуществующих биржах.

В таком случае потерпевший самостоятельно находит рекламу о подобном заработке в социальных сетях, сайтах, мессенджерах, после чего оставляет соответствующую заявку. Далее потерпевшему начинают поступать звонки с различных иностранных номеров. В ходе разговоров звонящие представляются менеджерами крупных брокерских компаний и под предлогом дальнейшего заработка посредством их платформы убеждают жертву зарегистрироваться на принадлежащей им трейдинг- платформе. В дальнейшем потерпевшему предлагается в качестве первого взноса для начала обучения внести небольшую сумму денежных средств. После того, как потерпевший внес так называемый первый взнос, ему начинают поступать звонки от других лиц, которые представляются личными брокерами. В дальнейшем, под предлогом более крупного заработка, потерпевшему предлагается внести более крупную сумму денежных средств. Для убедительности своих действий мошенники под видом вывода заработанных денежных средств с фальшивой трейдинг- платформы перечисляют потерпевшему незначительную сумму, тем самым убеждают потерпевшего в том, что он работает с реальной организацией. Также для того, чтобы окончательно убедить потерпевшего, мошенники посредством переписки, либо на электронную почту присылают копии несуществующих документов, фотографии с изображением удостоверений, сертификатов, лицензий, чаще всего на иностранном языке. Спустя время потерпевший не получает как перечисленные им денежные средства, так и фиктивно заработанные. В конечном итоге, когда потерпевший понимает, что был обманут, злоумышленники либо прекращают общение с ним, либо продолжают свои противоправные действия путем запугивания. Также к потерпевшему могут обращаться другие лица, которые представляются сотрудниками иностранной юридической фирмы,

занимающейся возвратом денежных средств, добытых мошенническим путем, однако данные лица также являются мошенниками. При этом на балансе приложения будут отображаться денежные средства, внесенные потерпевшим, однако в действительности доступа к данным денежным средствам потерпевший не имеет.

Для защиты от подобных мошеннических действий необходимо не доверять обещаниям лёгкого и быстрого обогащения, особенно если они исходят от незнакомых лиц или непроверенных источников. Важно тщательно изучать информацию о криптовалютных биржах, проверять их репутацию и лицензии.

Так, например, жительница г.п.Ушачи нашла, казалось бы, безобидное объявление в социальной сети, где предлагалось быстро заработать на онлайн-торгах. Женщина оставила заявку, после чего с ней связалась девушка, представившись наставником. Мошенница детально объясняла «тонкости» работы на фейковой бирже, для жертвы создали личный кабинет с виртуальными 15 тысячами долларов «стартового капитала». Но спустя несколько месяцев куратор сообщил, что все деньги потеряны из-за «неудачных инвестиций» и потребовал вернуть долг. Чтобы спасти ситуацию, женщина потратила личные сбережения, заняла деньги у знакомых и оформила несколько кредитов. В общей сложности она перевела мошенникам более 54 тысяч рублей.

В Республике Беларусь разрешено покупать и продавать криптовалюту за денежные средства только у криптобирж, являющихся резидентами Парка высоких технологий. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц являются незаконным и запрещается.

Интернет-адвокаты

Набирает популярность такая схема, как фиктивный возврат потерянных денежных средств. Мошенники выходят на связь с потерпевшими, которые ранее стали жертвами аферистов, обещают им помочь вернуть украденные средства. Мошенники позиционируют себя «юристами», «департаментом по возврату инвестиций».

ТОРГОВЫЕ ПЛОЩАДКИ И ИНСТАГРАМ

Также одним из самых распространенных способов совершения мошенничеств в глобальной сети Интернет является онлайн-торговля,

на Интернет-площадках и в группах в социальных сетях, таких как «Инстаграм», «ВКонтакте», «Телеграм», «Куфар» и т.д. Чтобы обмануть покупателей и продавцов, мошенники создают поддельные сайты, предлагая товары по слишком низким ценам, используя фальшивые отзывы для повышения доверия.

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.

ФИШИНГ

По-прежнему одной из самых распространенных схем хищения является фишинг - создание поддельных сайтов.

С учетом приближающейся поры долгожданных отпусков и путешествий. Граждане бронируют путевки, жилье, билеты, предвкушая долгожданный отдых. К сожалению, мошенники используют это в своей преступной деятельности, создавая поддельные сайты, имитирующие известные туристические агентства, авиакомпании или отели, предлагающие «выгодные» предложения.

Например, на этой неделе в РОВД обратилась женщина, которая в поисках доступного варианта для отпуска, наткнулась в Instagram на привлекательное объявление. Яркие фотографии, заманчивые цены и обещания незабываемого отдыха в Турции сделали своё дело. Недолго думая, они связались с продавцом, польстившись на выгодное предложение, совершили перевод денежных средств в сумме более 5000 рублей, не подозревая, что стали жертвой мошенников.

Если потерпевшие пытаются вернуть деньги, злоумышленники также могут воспользоваться и этим. Для получения возврата денежных средств - присылают ссылку на страницу для заполнения реквизитов банковской карты.

КТО ТАКИЕ ДРОПЫ?

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 интернет-банкинга, а также предоставить разовый СМС- код.

Поиск дропов

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.

Ответственность

Надо знать, что статьей 222 Уголовного кодекса 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. За предоставление своих личных данных для использования в мошеннических схемах предусмотрена административная ответственность по статье 12.35 Кодекса Республики Беларусь об административных правонарушениях.

Имеются факты, когда в преступную деятельность вовлекались несовершеннолетние.

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ

Запомните следующие правила:

- если незнакомый заводит беседу про ваши деньги, прекратите разговор;

- не доверяйте незнакомым и не выполняйте то, о чем они просят, даже если обещают помощь в сохранении денежных средств;

- не устанавливайте непроверенные программы на свои электронные устройства по указанию незнакомых;

- при совершении покупок в сети Интернет производите оплату только после получения товара и проверки его состояния;

- не забывайте, что мошенники могут представляться вымышленными данными, использовать для подтверждения личности фотографии чужих паспортов, чужие аккаунты в соцсетях, чужие абонентские номера.

- 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, наилучший способ общения - личная встреча с продавцом, осмотр товара на месте;

- 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;

- 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.

«Цифровая грамотность»

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

(Материал предоставлен Чашникским РОВД)