УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ УВД ВИТЕБСКОГО ОБЛИСПОЛКОМА

УТВЕРЖДАЮ
Начальник УПК КМ
УВД Витебского облисполкома
полковник милиции
А.Н.Гарус
«24» февраля 2025 г.

ПЛАН-КОНСПЕКТ
проведения профилактического выступления по линии противодействия киберпреступности

Тема: «Современные способы совершения киберпреступлений на территории Витебской области»

Витебск, 2025 г.

СОВРЕМЕННЫЕ СПОСОБЫ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ НА ТЕРРИТОРИИ ВИТЕБСКОЙ ОБЛАСТИ

Несмотря на принимаемые сотрудниками органов внутренних дел меры по противодействию киберпреступности, проблема остается актуальной и требует комплексного подхода. Современные технологии развиваются с неимоверной 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 непредосторожности. 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 (вишинг).

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 в формате *.арк.

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.

Так, например, с начала года зафиксированы неединичные случаи: мошенники посредством сети интернет, в мессенджере «Вайбер», представившись работником «МТС», под предлогом продления абонентского номера, завладевают персональными данными и СМС- кодами.

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:

Например, в текущем году в один из РОВД г.Витебска обратилась работница учреждения образования, которая сообщила, что на ее мобильный телефон, представившись сотрудником «Энергосбыта», позвонил незнакомый, под предлогом замены счётчиков завладел паспортными данными (ФИО, идентификационный номер, адрес места жительства). Также посредством сети интернет, в мессенджере «Вайбер» мошенническим путём, представившись сотрудником Национального банка, под предлогом прекращения оформления кредитов на её имя пытался завладеть денежными средствами на общую сумму 36 000 рублей.

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 рабочего одного из предприятий города Витебска посредством сети интернет, в ходе разговора в мессенджере «Телеграмм», мошенническим путем, представившись сотрудником правоохранительных органов, под предлогом оформления кредита для оказания помощи в разоблачении мошенника, преступники пытались завладеть денежными средствами в сумме 40 000 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. Как правило мошенники, имея фото или логотип крупной организации, создают 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 для трейдинга, которое было установлено по указанию мошенников будут отображаться денежные средства внесенные потерпевшим, однако в действительности доступа к данным денежным средствам потерпевший не имеет.

Так, например, в г. Орша 36-летний рабочий одного из предприятий в социальных сетях нашел рекламное предложение о выгодном вложении денежных средств, перейдя по ссылке он заполнил анкету, где указал свои личные данные. Сразу после этого с ним связался специалист по трейдингу и быстро ввел в курс начинающего инвестора. Мужчина оформил на себя два кредита, занял приличную сумму и перевел на указанный мошенниками счет более 26 000 рублей. Затем под предлогом оплаты различных налогов и пошлин за вывод денежных средств, оршанца убедили перевести еще более 10 000 рублей.

На момент, когда оршанец осознал, что его обманывают, он уже успел перевести мошенникам более 40 000 рублей.

Следует отметить, что мошенники для совершения преступлений изучают свою жертву, собирают в сети Интернет данные о ней и ее интересах, окружении и прочем. Имея образец голоса или фото знакомых, могут создавать фейковые текстовые или видеосообщения.

Например, в 2024 году зарегистрировано несколько подобных фактов. В мессенджере мошенники создали учетную запись руководителя госорганизации и от его имени написали сотруднице, что поступили списки работников, которые подозреваются в финансировании ***экстремистских*** *формирований, и вскоре, возможно, в жилье женщины проведут обыск и* ***изымут незадекларированные*** *денежные средства. Женщина очень испугалась за свои деньги, потому что доверяла руководителю. Далее мошенники от имени ее руководителя предложили пообщаться с Начальником Департамента финансовых расследований области, который в свою очередь связал ее со следователем. В течение трех дней женщина пребывала в страхе за свои сбережения. Чтобы сохранить их мошенники «посоветовали» перевести их на якобы специальный защищенный счет. Также женщина за неделю получила кредит, обналичила его и перевела на тот же счет, откуда вскоре все деньги в сумме 55 тысяч рублей были похищены.*

Не стоит забывать, что с целью получения личных данных владельцев и счетов, мошенники создают страницы-клоны банков, сайтов театров, кальянных и инвестиционных (торговых) 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**» (ссылка-приглашение «**t.me/cifgram**»), где на регулярной основе публикуется актуальная информация о способах совершения киберпреступлений и методах противодействия им.

Управление по противодействию киберпреступности
КМ УВД Витебского облисполкома