

Об отдельных вопросах противодействия преступлениям, совершаемым с использованием возможностей глобальной компьютерной сети Интернет

В современном мире наблюдается активное внедрение и совершенствование электронных информационных систем, а также автоматизация множества процессов. В настоящее время сложно выделить сферу деятельности в которой бы не применялись информационные технологии.

Бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений, то есть правонарушений, при совершении которых средства компьютерной техники выступают как предмет преступного посягательства.

За восемь месяцев 2026 года территориальным подразделением Следственного комитета Октябрьского района г. Минска возбуждено 872 уголовных дела, из которых 325 о преступлениях в сфере высоких технологий. При этом, большинство противоправных деяний совершаются путем использования социальной инженерии: «вишинг» и «фишинг».

Как правило, киберпреступники выдают себя за людей, действующих на законных основаниях организаций и учреждений, чтобы обманом вынудить граждан раскрыть личную информацию и предоставить преступникам деньги, товары и/или услуги.

Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные, имущество и денежные средства граждан.

Наиболее распространенным видом проявления киберпреступности является хищение денежных средств с карт-счетов граждан. Причем в большинстве случаев эти преступления становятся возможны в результате беспечных действий потерпевших, предоставивших реквизиты доступа к своим банковским счетам. Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих способов:

1. Фишинг (от англ. fishing — «рыбная ловля»). В качестве своеобразной удочки преступники используют специально созданный интернет-сайт с формой ввода на нем реквизитов доступа к банковскому счету, а в качестве наживки — некий сообщенный потерпевшему предлог для перехода на этот сайт и заполнения платежных реквизитов.

Пример маскировки под площадку Kufar.by

На данный момент известно о нескольких типичных схемах мошенничества. Они направлены как на продавцов, так и на покупателей товаров.

Схема обмана продавцов № 1 (Предварительная оплата)

Преступник находит продавца на официальной площадке объявлений, копирует его контактные данные, но на площадке не пишет, поскольку пересылка фишинговых ссылок там невозможна. Ищет номер продавца в мессенджерах или пишет в соцсетях, представляясь якобы покупателем с Куфара. Говорит, что уже совершил предоплату. Высылает продавцу ссылку на поддельную страницу, где продавцу нужно ввести номер своей карты для того, чтобы получить деньги. Среди данных, которые просит злоумышленник: номер карты, имя держателя, срок действия, CVV-код на оборотной стороне карты.

Иногда мошенник также просит продавца предоставить SMS-код подтверждения платежа, ссылаясь на то, что перевел предоплату и хочет убедиться, что она поступила на счет продавца. С помощью собранных данных мошенник может попытаться перевести с карты жертвы некую сумму денег, и, если на счете будет достаточно средств, ему это удастся.

Схема обмана продавцов № 2 (Предварительная оплата)

Если предыдущая схема успешно сработала, мошенник может повторно сам связаться с покупателем или представиться службой поддержки и сказать, что произошла ошибка. Чтобы вернуть ошибочно переведенные средства, он предложит перейти на фишинговый сайт и снова ввести данные своей карты. Если продавец это сделает, мошенник может повторно списать деньги.

Схема обмана покупателей № 1 (Доставка базовая)

Преступник выставляет товар на официальной площадке объявлений по крайне выгодной цене. Когда потенциальный покупатель пишет ему, преступник убеждает перейти в мессенджер или социальную сеть под предлогом того, что там удобнее общаться. Во время общения мошенник уговаривает покупателя на предоплату или доставку под любым предлогом: уехал из города, нет времени. Чтобы развеять сомнения покупателя, говорит о новой услуге холдирования средств, которая появилась на Куфаре: если доставки не будет, Куфар автоматически вернет средства на карту. Высылает покупателю ссылку на поддельную страницу, которая имитирует страницу сервиса «Куфар Доставка» или интернет-банкинга, где нужно ввести данные карты, чтобы совершить предоплату. В качестве данных карты покупателя просят заполнить номер карты, имя держателя, срок ее действия, CVV-код (3 цифры на оборотной стороне карты). В некоторых случаях злоумышленник может попросить назвать проверочный код из SMS-уведомления банка. Как только пользователь вводит данные своей карты, с нее списываются деньги, посылка, естественно, не приходит и средства не возвращаются.

Схема обмана покупателей № 2 (Доставка повторная)

После того, как предыдущая схема полностью реализована, и покупатель начинает подозревать, что его обманули, мошенник повторно связывается с покупателем. Говорит, что произошла ошибка; товар уже забрали (или передумал подавать), готов вернуть деньги. Высылает ссылку на поддельную страницу возврата средств, где покупателю нужно ввести все те же данные своей карты и точную сумму, которую ему должны вернуть. После того, как покупатель повторно вводит данные своей карты, с его счета повторно списываются деньги.

Схема обмана покупателей № 3 (Возврат средств)

После того, как мошенник реализовал схему «Доставка», он пишет пострадавшему покупателю, представляется службой поддержки Куфара. Говорит, что посылка была не доставлена, извиняется и рассказывает про возможность возврата средств за посылку. Присылает ссылку на фишинговую страницу, где покупателю снова нужно ввести данные своей карты и сумму, которая соответствовала сумме предыдущего списания. После того, как покупатель повторно вводит данные, мошенник снова крадет деньги с банковского счета.

Схема обмана покупателей № 4 (Мошенничество с накладными)

Преступник выставляет товар по очень выгодной цене на официальном сайте. Когда потенциальный покупатель пишет ему на Куфаре, под любым предлогом предлагает перейти в мессенджер. Уговаривает отправить товар по почте. При этом мошенник специально создает ажиотаж вокруг объявления. Он может говорить, что буквально на днях уезжает из города, или что товар готовы купить другие покупатели. Продавец говорит, что можно оплатить товар уже после того, как он его отправит, при этом готов предоставить доказательства. Если покупатель соглашается, в качестве доказательства отправки мошенник высылает ссылку на поддельную страницу трекинга посылки или скан поддельного документа об оплате. Минимальное знание фотошопа позволяет преступнику симитировать квиток любой службы доставки, будь то СДЭК, Белпочта или любая другая компания. После того, как покупатель поверил, что посылка отправлена, мошенник присылает ссылку на фишинговую страницу, где

нужно оформить перевод суммы за товар. Как только пользователь вводит данные своей карты, с его счета списываются деньги, а посылка, естественно, не приходит.

Так, к примеру, в производстве Октябрьского (г. Минска) районного отдела Следственного комитета Республики Беларусь (далее – Октябрьского РОСК) находится уголовное дело, возбужденное по ч. 1 ст. 212 УК по факту хищения денежных средств потерпевшей в сумме 300 рублей путем модификации компьютерной информации. Установлено, что потерпевшая на торговой площадке «Куфар» нашла объявление о сдаче в аренду жилья. Связавшись с «продавцом» ей было предложено продолжить обсуждение аренды в мессенджере «Telegram». Для оформления сделки злоумышленник отправил потерпевшей ссылку, перейдя по которой последняя ввела номер выпущенной на ее имя банковской платежной карты, CVV код, и далее, по указанию неустановленного лица сообщила пришедший в смс-сообщении проверочный код. В дальнейшем, в считанные минуты после предоставления указанных сведений, со счета банковской платежной карты потерпевшей были списаны все имеющиеся денежные средства в сумме 300 рублей.

2. Вишинг (от англ. voice fishing – «голосовой фишинг» или «голосовая рыбная ловля»). Данный способ выражается в осуществлении злоумышленником звонка с использованием подмены номера (IP-телефония), что в свою очередь позволяет использовать номера, которые похожи на номера банков с официальных сайтов, на абонентский номер потерпевшего или в его аккаунт в мессенджере (в основном это Viber или Telegram).

В ходе голосового общения преступник представляется работником банка или правоохранительного органа (МВД, КТБ, ДФР, Следственного комитета) и под вымышленным предлогом (пресечение подозрительной транзакции, повышение уровня безопасности пользования картой, перепроверка паспортных данных владельца банковского счета и т.д.) выясняет у потерпевшего сведения о наличии банковских платежных карт, сроках их действия, CVV-кодах (трехзначный код на обратной стороне карты), паспортных данных, SMS-кодах с целью хищения денежных средств.

Нередки также случаи, когда злоумышленники, представляясь сотрудниками правоохранительных органов под вымышленным предлогом, в частности о причастности потерпевшего к различным преступлениям, сообщают о намерении провести обыск у него по месту жительства с целью изъятия всего имущества. После чего, в качестве якобы акта милосердия, злоумышленники предлагают испуганному потерпевшему сохранить свои денежные средства путем их перевода на «безопасный счет», то есть якобы их задекларировать, и по окончании проведения проверки или расследования возратить, на что потерпевшей соглашается, указывает имеющуюся в наличии сумму денежных средств и по указанию якобы сотрудника правоохранительных органов переводит денежные средства на счет злоумышленника.

Если стали жертвой мошенников:

Если ввели данные банковской карты, то необходимо в срочном порядке произвести ее блокировку, позвонив в банк либо в интернет-банкинг, либо три раза введя неверный пароль, с последующей ее заменой.

Если ввели авторизационные данные от интернет-банкинга, то необходимо немедленно звонить в банк и сообщить о компрометации учетных данных от интернет-банкинга.

В случае необходимости обратиться в правоохранительные органы с заявлением о мошенничестве.

Например, в производстве Октябрьского РОСК находится уголовное дело, возбужденное по ч. 4 ст. 209 УК по факту завладения путем мошенничества денежными средствами потерпевшего в сумме 53 000 рублей. Установлено, потерпевшему в мессенджере «Viber» с абонентского номера белорусского оператора связи поступил звонок от неустановленного лица, представившегося сотрудником Национального банка, который поинтересовался, имеются ли у него на счету денежные средства. Услышав утвердительный ответ, злоумышленник предложил защитить денежные средства от мошенников путем их передачи сотруднику банка для декларирования. В последующем, потерпевший, действуя по

указанию якобы сотрудников банка, снял со своего счета все денежные средства и передал их курьеру, неосведомленному о совершаемом преступлении.

3. Шантаж. В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. К примеру, получив несанкционированный доступ к интернет-ресурсам (страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам) и, завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет.

Так, в производстве Октябрьского РОСК находится уголовное дело, возбужденное по ч. 1 ст. 208 УК по факту вымогательства. Установлено, что с несовершеннолетней потерпевшей в ходе переписки в Интернет-мессенджере «Telegram» связался пользователь «@Swags_NFTs», пояснил, что завладел ее профилем и потребовал 400 рублей за то, что не будет надоедать звонками ее знакомым и близким.

Или, к примеру, в производстве указанного районного отдела находится уголовное дело, возбужденное по ч. 1 ст. 208 УК по факту вымогательства. Установлено, что потерпевшая познакомилась в социальной сети «ТикТок» с «Владом», после чего они стали поддерживать общение. В ходе переписки «Влад» убедил потерпевшую передать ему данные своей учетной записи в мессенджере «Telegram», после чего осуществил вход в вышеуказанную учетную запись и обнаружил ее интимные фотографии и видеозаписи. В последующем «Влад» сообщил потерпевшей, что в случае не перечисления ему денежных средств в сумме 500 долларов США, он распространит в глобальной сети Интернет обнаруженные интимные материалы.

4. Иные мошенничества.

Также можно выделить еще несколько типов мошенничества, которые в недавнем прошлом часто успешно использовались на территории Республики Беларусь:

- просьба пополнить счет определенного номера мобильного телефона или платежной карты в виде «Мама,полни счет на 20 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!»;

- звонок с номера друга или родственника, в котором собеседник утверждает, что он сотрудник правоохранительных органов, просит вознаграждение, обещая предотвратить возбуждение уголовного дела в отношении близкого человека;

- звонок о необходимости продлить срок договора по оказанию услуг электросвязи, замены домофона, где мошенник выясняет паспортные данные жертвы, просит сообщить пришедшие в SMS-сообщении коды, а в последующем от имени жертвы оформляются банковские платежные карты, через счета которых мошенники переводят похищенные у иных лиц денежные средства, либо мошенники получают доступ к счету банковской платежной карты жертвы, с которого в дальнейшем несанкционированно похищают денежные средства;

- отклик мошенника на заявку жертвы о трудоустройстве, подработке, где мошенники предлагают якобы выгодные условия по трейдингу, для чего жертвы, как правило, оформляют кредиты, перечисляют денежные средства на счета, криптокошельки, доступ, к которым самостоятельно предоставляют мошенникам, которые, получая доступ к счету (криптокошельку) якобы обучают таким образом трейдингу, а в действительности похищают денежные средства, отправляя жертвам картинки якобы успешного трейдинга;

- когда приходит SMS-сообщение о некоем выигрыше, после чего абоненту предлагают отправить платное сообщение в ответ или отправить небольшую сумму на банковскую карту для получения «выигрыша»;

- когда приходит SMS-сообщение с гиперссылкой, пройдя по которой пользователь запускает процесс скачивания вируса;

- когда поступает звонок от «представителя сотового оператора», во время которого злоумышленники предлагают перерегистрировать SIM-карту, при этом пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного телефона списываются деньги;

- когда приходит SMS-сообщение или поступает звонок, в ходе которого сообщается, что абонент не оплатил штраф, после этого человеку предлагается произвести его оплату, перечислив деньги на «специальный» расчетный счет или пополнив банковский счет;

- когда приходит SMS-сообщение с информацией о том, что платежная карта заблокирована, и указывается номер, по которому можно получить справку или помощь; после звонка у абонента запрашивают PIN-код, CVV-код (трехзначный код на обратной стороне карты), номер карты и другие данные, необходимые для снятия денег с банковского счета.

Какие способы мошенничества бывают в отношении юридических лиц и индивидуальных предпринимателей?

Киберпреступления причиняют ущерб не только гражданам. Часто действия злоумышленников направлены на завладение денежными средствами юридических лиц (предприятий, учреждений и организаций) и индивидуальных предпринимателей. Однако и здесь главным условием, дающим возможность совершения подобных злодеяний, является человеческий фактор, т.е. грубые ошибки, допускаемые работниками: от руководителей до секретарей, бухгалтеров и менеджеров. Все чаще потерпевшими становятся юридические лица и индивидуальные предприниматели, которые осуществляют деятельность при помощи зарубежных контрагентов. Среди наиболее типичных форм посягательств хакеров на денежные средства и охраняемую информацию юридических лиц являются ВЕС-атаки (от англ. business email compromise – «компрометация бизнес-переписки»). Реализация подобной схемы хищения возможна посредством получения несанкционированного доступа к электронной почте одной из сторон сделки. В этой ситуации злоумышленники обладают информацией о предмете, условиях договора и могут вести переписку, не вызывая подозрений (в случае необходимости ими направляются дополнительное соглашение, счет-проформа (инвойс) с измененными реквизитами банковского счета и контактными данными представителей фирмы путем их «наложения» на подготовленные ранее и сохраненные в сообщениях документы). Кроме того, имеются случаи, когда от имени белорусских субъектов хозяйствования после взлома их корпоративной почты в адрес зарубежных партнеров также направлялись письма, счета-проформы с измененными банковскими реквизитами. В результате денежные средства, причитающиеся белорусским предприятиям за произведенную (поставленную) продукцию, переводились на счета мошенников. Также возможна ситуация, когда после согласования существенных условий контракта с зарубежным партнером, а в отдельных случаях и его «подписания, на электронную почту организации (предприятия) преступниками направляется сообщение якобы от имени сотрудника иностранного контрагента об изменении реквизитов обслуживающего банка и необходимости перечисления денежных средств на новый счет. При этом адрес электронной почты мошенников имеет существенное сходство с реальным, что часто остается незамеченным. Последующая переписка уже осуществляется с киберпреступниками. Далее под предлогом оплаты товаров иностранных компаний и вследствие предоставления по электронной почте ложных банковских реквизитов на счета мошенников перечисляются денежные средства со стороны субъектов хозяйствования как государственного, так и частного сектора экономики.

К примеру, в производстве Октябрьского РОСК находится уголовное дело, возбужденное по ч. 4 ст. 209 УК по факту завладения путем мошенничества денежными средствами юридического лица. Установлено, что представитель юридического лица договорился с представителями ООО «Эксперт Групп» (юридическое лицо на территории Российской Федерации) о поставке оборудования. Все договоренности между представителями организаций осуществлялись исключительно дистанционно посредством конференцсвязи и переписки по электронной почте. При этом представитель белорусской организации российскую организацию на предмет ее существования через налоговые органы

Российской Федерации не проверял, а перечислил предварительную плату за оборудование по реквизитам, указанным в договоре. После перевода денежных средств представители ООО «Эксперт Групп» перестали выходить на связь, оборудование поставлено не было.

Для того чтобы обезопасить себя и свои денежные средства, необходимо соблюдать следующие правила:

1. Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

2. В случае поступления звонка от «сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

3. Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете. Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

4. В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, ведь все подобные вопросы нужно решать в отделении банка, а не по телефону.

Внимание! Помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp).

5. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, обязательно проверяя доменное имя ресурса в адресной строке браузера.

6. Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам; это же относится к фотографиям и иным видам информации конфиденциального характера.

7. Следует воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

8. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт по просьбе пользователей сети Интернет.

9. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам необходимо использовать сложные пароли, исключающие возможность их подбора. Стоит воздержаться от следующих паролей: дат рождения, имен, фамилий, т.е. тех, которые легко вычислить из общедоступных источников информации (например, социальных сетей).

10. При составлении платежных документов важно проверять платежные реквизиты получателя денежных средств.

11. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «Друзья», с просьбами о предоставлении реквизитов банковских платежных карточек не следует отвечать на подобные сообщения, необходимо связаться с данными пользователями напрямую посредством иных средств связи. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

12. Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров, переходить по ссылкам в сообщениях о призах и выигрышах.

13. Необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему, установить антивирусную программу не только на персональный компьютер, но и смартфон, планшет, и регулярно обновлять ее.

14. Следует ознакомить с перечисленными правилами безопасности своих родственников и знакомых, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

Какие советы можно дать юридическим лицам, чтобы обезопасить себя от мошенничества?

1. Выработать четкий план реагирования и ознакомить работников с перечнем сведений, относящихся к коммерческой, служебной и иной тайне.

2. Исключить в своей деятельности использование бесплатных почтовых сервисов, а также принимать дополнительные меры защиты корпоративной электронной почты (подключение двухфакторной аутентификации, соблюдение требований к сложности пароля и периодичности его смены, использование антивирусного программного обеспечения).

3. Неукоснительно соблюдать правила пользования системой дистанционного банковского обслуживания.

4. Создавать резервные копии данных и хранить их на съемных носителях.

5. Проверять правильность адреса электронной почты контрагента при получении и отправке сообщений, а также поддерживать контакт с его представителем и согласовывать ключевые вопросы дополнительно посредством иных средств связи (телефонных переговоров, использования факсимильной связи, мессенджеров и проч.).

6. Не использовать рабочие устройства в личных целях, а служебные ящики электронной почты — для регистрации на торговых и развлекательных онлайн-площадках.

7. Наладить строгий действенный контроль за соблюдением утвержденных мер информационной безопасности (соответствие программного обеспечения, проверка отсутствия несанкционированного доступа к внешним информационным ресурсам и т.д.).

Обращаем внимание, что в Республике Беларусь появился уникальный сервис – Проверь.Бел, который помогает быстро выявлять мошенников в социальных сетях и мессенджерах. Получили сообщение от незнакомца? Вам предлагают перевод, покупку или «выгодную» сделку? Не спешите доверять – сначала проверьте. Введите имя аккаунта или ссылку на профиль на сайте Проверь.Бел – и сразу узнаете, есть ли он в базе мошеннических профилей. Одна минута проверки может уберечь вас от потери денег, обмана и лишних проблем.