БУДЬТЕ ВНИМАТЕЛЬНЫ!!!

22.04.2025

Наиболее распространенные способы хищения имущества путем модификации компьютерной информации и типичных последствиях их применения.

1. Обман потерпевшего под предлогом продажи вещей на интернет-площадке.

На торговых интернет-площадках правонарушитель находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хочет приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности лично за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на банковскую платежную карточку (далее - БПК) пользователя и после того, как он соглашается, высылает в его адрес ссылку с фишинговой (поддельной) страницей сайта определенного банковского или иного учреждения (страница может быть визуально схожа со страницей интернет-банкинга и отличаться только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится на поддельной странице интернет-банкинга. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свои реквизиты БПК, логин и пароль от интернет-банкинга либо паспортные данные, а также код из смс-сообщения. После ввода указанной информации пользователю сообщается об ошибке либо невозможности совершить платеж. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка или ином ресурсе, получая тем самым доступ к денежным средствам жертвы и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может ее осуществить, и просит повторить действия с какой-то другой карточкой (родственников или знакомых).

2. Обман поперевшего под предлогом покупки вещей на интернет- площадке.

На торговых интернет-площадках злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и преднамеренно устанавливает цену ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности лично встретиться для передачи имущества, предлагает воспользоваться курьерскими услугами (например, «Доставка Куфар», «Белпочта (ЕМС)», «Курьерская служба (СДЭК)»). При согласии покупателя правонарушитель высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где предлагается ввести реквизиты БПК для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также код из смс-сообщения. После ввода данной информации пользователю обычно сообщается об ошибке либо сайт перестает загружаться («зависает»). В это время всю введенную информацию видит злоумышленник и вводит ее на действительном сайте банка, получая доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, он сообщает пользователю, что по техническим причинам не может ее осуществить, и просит повторить указанные действия с какой-то другой карточкой (родственников или знакомых).

3. Обман потерпевшего под предлогом оказания помощи от имени банковских работников.

На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника. Как правило, при этом последний пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним, либо использует для осуществления звонка мессенджер (например, Viber), где у вызывающего абонента имеется ярлык с логотипом банковского учреждения. Далее он представляется сотрудником банка (может назвать пользователя по имени и отчеству, а также

сообщить часть номера БПК либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков или оформлении кредитов на имя потерпевшего. Когда потерпевший отвечает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя назвать отдельные реквизиты БПК либо паспортные данные и сообщает, что высылает в адрес пользователя смс-сообщение с кодом, который необходимо назвать после звукового сигнала. В это время все полученные сведения злоумышленник вводит на сайте банка, получает доступ к денежным средствам пользователя и совершает их хищение. Следует помнить, что запрашиваемая преступником информация сотрудникам банка не требуется ни при каких обстоятельствах и они не будут узнавать о ней у клиента.

4. Обман потерпевшего под предлогом покупки билетов в кино, театр, бронирования кальянных, саун и пр. (так называемая схема «Антикино»).

Киберпреступники с фейковых аккаунтов на различных сайтах, представляясь девушками, знакомятся с мужчинами и предлагают продолжить общение в мессенджерах. Для убедительности они направляют собеседникам фотографии и голосовые сообщения, ведут беседы по телефону. Затем мошенники присылают фишинговую ссылку на сайт, например, несуществующего кинотеатра, в котором предлагают провести время. Мужчинам необходимо забронировать места и все оплатить. Потерпевшие вводят реквизиты своих ВПК, тем самым предоставляя мошенникам полный контроль над карт-счетами. Таким образом злоумышленники завладевают деньгами. При попытке обратиться в службу поддержки сайта обманутые граждане снова попадают на киберпреступников, что препятствует своевременному обращению в правоохранительные органы.

5. Обман потерпевшего под предлогом продления срока действия SIM- карты.

На телефон поступает звонок от неизвестного, представляющегося официальным лицом сотовой компании, которое сообщает об окончании срока действия SIM-карты. Для его продления мошенники просят назвать код из смс- сообщения, который приходит на телефон. Так они пытаются получить доступ в личный кабинет на сайте оператора связи, после чего устанавливают переадресацию на контролируемый преступниками номер. Иногда для вхождения к ним в доверие предлагают перейти потерпевшим по фейковой ссылке.

6. Обман потерпевшего под предлогом оказания содействия в получении посылки на «Белпочте».

Потерпевшему направляются сообщения о пришедшей посылке, которую можно получить после заполнения недостающей информации, перейдя по ссылке. В реальности же последняя является фишинговой, а ввод данных позволяет мошенникам получить доступ к карт-счету и похитить деньги.

7. ***Обман потерпевшего под предлогом оказания помощи его родственнику или близкому.***

На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника, который сообщает, что родственник жертвы попал в неприятную историю (например, он участник ДТП, ему грозит тюрьма, он находиться в больнице). После этого трубку берет якобы врач (следователь, милиционер, прокурор) и говорит, что срочно нужны деньги, чтобы оплатить дорогостоящее лечение или дать взятку («откупиться»). В процессе диалога потерпевший беспрекословно выполняет требования мошенника: в некоторых случаях устанавливает на своем телефоне программу AnyDesk, RustDesk, с помощью которых мошенник отслеживает и контролирует все его действия, выведывает конфиденциальную информацию доступа к банковскому счету, вынуждает оформить и переоформить кредит либо сообщает, что приедет курьер, которому следует передать наличные деньги. Таким образом, в результате мошеннических действий потерпевший лишается денежных средств.

8. Обман потерпевшего под предлогом временного заимствования денег.

После несанкционированного доступа к страницам пользователя в социальных сетях злоумышленник рассылает от его имени лицам, находящимся в разделе «Друзья», сообщения

с просьбой об оказании помощи, выражающейся в переводе денежных средств, для чего используются различные предлоги: «Привет, не мог бы ты одолжить мне денег? Отдам через пару дней», «Привет, положи, пожалуйста, 10 рублей на телефон, я отдам», «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)?». Далее преступник входит в доверие к неравнодушным пользователям и якобы для перевода денежных средств просит сообщить реквизиты БПК и коды из смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, не догадавшийся о преступности его намерений, сообщает запрашиваемые сведения, ввиду чего злоумышленник получает доступ к денежным средствам жертвы и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, то есть фактически уже похитив деньги с одной карты, злоумышленник часто сообщает, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой карточкой (родственников или знакомых), чтобы продолжить хищения с других банковских счетов.

Все приведенные примеры показывают, что мошенники используют фактор неожиданности и создают для жертвы максимально неудобные, ограниченные по времени условия для анализа происходящего. Обычно их интересует номер БПК, логин и пароль от кабинета пользователя, коды из смс- сообщения.

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

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты БПК, расчетных счетов, секретные (CVC/CVV-коды, данные касательно последних платежей и срока действия пластиковых карточек третьим лицам;

подключить и использовать технологию «3D Secure», которая обеспечивает безопасность платежей в сети Интернет, позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества. При использовании этой технологии держатель БПК подтверждает каждую операцию по своей карточке специальным сеансовым паролем, который он получает в виде смс-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученных в смс-сообщениях сеансовых паролей для подтверждения операций, а также своих БПК, каким бы то ни было способом;

вводить секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https:/!, а не http.VA

производить регулярный мониторинг выполненных операций, используя раздел с историей платежей, контролировать свои списания:

использовать дополнительный уровень безопасности (системы многоуровневой аутентификации, смс-информирование о расходных операциях);

подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Изменять пароль каждые 2-4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга;

не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или если для входа на сайт используется компьютер общего доступа;

устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

привязать к MAC или IP-адресу вход в личный кабинет на сайте интернет- банкинга;

выкладывать фотографию ВПК в сеть Интернет, поскольку имеющихся на изображении сведений может быть достаточно для совершения операций с использованием этих данных без ведома владельца.

Источник: Гродненский межрайонный отдел Следственного комитета Республики Беларусь

НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА

1. **QR-коды**
   Схема кражи денег через расклеенные в подъездах QR-коды. Аферисты маскируют их под объявления, а также предлагают оплатить по ним товар.
   Результат: сканируя код, человек либо попадает на мошеннический сайт, либо его смартфон начинает скачивать вредоносную программу.
2. Лёгкие деньги.
   В социальных сетях распространяются многочисленные ссылки на формы для получения доступа к информации о быстром заработке. Обещания легких денег без усилий заставляют людей действовать импульсивно.
   Результат: денег нет, но Вы держитесь.
3. Звонки с целью анкетирования.

4. Запись на подачу визы
   Злоумышленники обманывают заявителей, обещая раннюю запись на подачу визы за дополнительную плату. Под видом посредников визовых центров запрашивают персональные данные и просят оплатить услугу, при этом осуществляя коммуникацию через мессенджеры и социальные сети.
5. Фейковые ИИ-сервисы.
   Это могут быть даже чат-боты на базе ИИ. Когда пользователь задает боту вопросы, тот в ответ может запросить паспортные данные или номер карты якобы для проверки личности или оказания услуг.
   Результат: пропадают данные и деньги.
6. В Интернете распространяется фальшивая ссылка, которая выдает себя за сайт сети аптек «Добрыя лекі». На этом фишинговом ресурсе предлагается заполнить форму для получения скидки «на весь ассортимент» лекарств. В форме просят указать ваше имя и номер телефона, а затем вам может позвонить «менеджер»
7.

Внимание!
Способы интернет-мошенничества!

Покупки через Интернет – это без сомнения очень удобно. Сфера Интернет-услуг расширяется, доходы сетевых ритейлеров растут, а люди все чаще предпочитают заказ товаров в сети походам по магазинам. Однако удобство Интернет-технологий распространяется не только на продавцов и покупателей. Мошенники также по достоинству оценили новые формы торговли и активно используют их своих целях.

Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег мы рекомендуем вам обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов.

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

На что следует обратить внимание? Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.

На что следует обратить внимание? Создание Интернет-магазина – дело нескольких часов, изменение его названия и переезд на другой адрес – дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

На что следует обратить внимание? Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия.

На что следует обратить внимание? Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы сделки. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие.

На что следует обратить внимание? Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки.

Если под их описание подходят два или более признака, мы настоятельно рекомендуем вам воздержаться от контактов с данным продавцом или магазином.