СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ, ИНФОРМАЦИЯ ОБ ОТВЕТСТВЕННОСТИ ЗА СОВЕРШЕНИЕ ТАКИХ ПРЕСТУПЛЕНИЙ

Последние несколько десятилетий в мире отмечается бурный рост компьютерных технологий. Практически все трудоспособное население страны, так или иначе вовлечено в активности, связанные с вычислительными ресурсами, чаще всего происходящими в сети Интернет. Проникновение Интернет активностей в молодежную среду специалистами также оценивается как близкое к 100%. На фоне развития компьютерных технологий отмечается и значительный рост преступлений с ними связанных. **Более 90% из выявленных преступлений составляют хищения путем использования компьютерной техники.** Также отмечается рост количества преступлений в сфере информационной безопасности.

В дальнейшем прогнозируется, что развитие IT-отрасли и финансово-кредитной сферы, будут способствовать сохранению тенденции увеличения числа преступлений по направлению деятельности в сфере высоких технологий.

Статья 212. Хищение путем использования компьютерной техники.

Необходимо отметить, что ответственность за деяния, предусмотренные ст.212, наступает с 14-летнего возраста. В зависимости от суммы максимальное наказание варьируется от 3 до 12 лет лишения свободы.

В настоящее время участились случаи совершения противоправных действий, когда мошенники осуществляют звонки с использованием подмены номера (IP-телефония), что в свою очередь позволяет использовать номера, которые похожи на номера банков с официальных сайтов. **Также для осуществления звонков используется мессенджер «Viber»** с изображением логотипа банковского учреждения, данный тип мошенничества называется **«ВИШИНГ».**

При установлении контакта с потенциальной жертвой **мошенники представляются сотрудниками банковского учреждения**, сообщают о попытках совершения подозрительных операций по счету, предлагают подтвердить их легитимность. После чего завладевают реквизитами платежных карточек (номер, срок действия карточки, CVV/CVC-код),

СМС-кодами, направляемыми от имени банковского учреждения.

Что необходимо знать гражданам в следующих случаях:

1) Поступают звонки с анонимного номера или номера схожего с номером банка.

Сотрудники банка не вправе выяснять в ходе телефонной беседы конфиденциальные сведения о клиенте (полный номер банковской платежной карты, срок ее действия, CVV-код, личный номер паспорта клиента, содержание СМС-сообщений от банка, и т.п.).

2) Собеседник просит вас скачать какие-либо приложения с магазина приложений “Play Market” или “App Store”.

Сотрудники банка никогда не просят устанавливать какие-либо приложения, так как программы, предлагаемые для скачивания «лжебанкирами», являются программами удаленного доступа и управления компьютерами и другими устройствами под управлением Windows, MacOS и Linux.

3) СМС якобы от банка приходит в новую переписку.

Не спешите переходить по ссылкам в сообщениях, предоставленных якобы банком.

4) Собеседник не может ответить на простые вопросы, при условии того, что настоящий сотрудник банка видит на экране компьютера всю информацию о клиенте, которая есть в базе банка.

Если собеседник не готов ответить на простой вопрос, например, назвать остаток по карте или последнюю операцию, то вероятно это мошенник.

5) Собеседник спрашивает данные карты или СМС-код.

Смс-код — один из главных паролей. Сотрудники банка никогда его не спросят, так же как и CVV на обратной стороне карты.

6) Вам обещают выгоду без усилий.

Чтобы завлечь жертву, мошенники обещают солидный доход быстро и без усилий: суперприбыльную работу, беспроигрышные конкурсы, курсы, которые сделают всех богатыми. Но мошенники могут взять предоплату за обучение и пропадут. Или посулят приз и выманят у вас данные карты якобы для перевода выигрыша.

7) Собеседник торопит вас или пытается переубедить.

Сотрудник банка никогда не будет настаивать или торопить клиента.

8) Ошибки в сообщении.

У банка есть бдительные редакторы, а вот мошенники пишут с ошибками. Не дайте неграмотному преступнику вас обмануть.

9) Имя отправителя написано неправильно.

Мошенники регистрируют адреса, похожие на названия банков.

Тут срабатывает особенность восприятия: мы считываем смысл слов даже, если буквы в них перепутаны. Когда приходит такое смс, вас должно насторожить ещё и то, что сообщение оказалось в новой переписке.

ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ:

Если вы хотите убедиться в надёжности собеседника, спросите его имя, а после перезвоните в банк по официальному номеру и попросите переключить на человека, который вам звонил.

 Если не уверены в собеседнике, попросите его назвать номер карты или остаток на счёте.

 Не паникуйте, если вам сообщают о блокировке счета. Позвоните в банк по номеру, указанному на сайте или на карте.

 Не обращайте внимание на обещания лёгких денег или выгоды без усилий.

 Если собеседник торопит вас или спрашивает смс-код, то вы говорите с мошенником!

 Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.

Вторая разновидность мошенничества называется «ФИШИНГ».

Целью данной разновидности мошенничества является получение не только учетных данных от каких-либо сервисов (логин и пароль), но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2 код). Это достигается путем направления пользователю в мессенджерах либо по электронной почте от имени известных брендов ссылки на сайт, внешне не отличимый от официального. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, а также реквизиты банковской платежной карты,

что позволяет в дальнейшем мошеннику получить доступ к аккаунтам и банковским счетам.

Пример маскировки под площадку Kufar.by

На данный момент известно о 6 типичных схемах мошенничества. Они направлены как на продавцов, так и на покупателей товаров.

Схема обмана продавцов № 1 (Предоплата)

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 СМС-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 (Предоплата)

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 СМС-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 сымитировать 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.

Рекомендации:

1. К любым операциям, производимым с использованием Вашей банковской карты, относится максимально внимательно и осторожно. Терять бдительность никогда нельзя.

2. Для оплаты покупок в Интернете завести отдельную карту с отдельным счетом и не хранить на ней много денег.

3. Если Вам прислали ссылку на почтовый ящик, в мессенджер или SMS-сообщением, то, независимо от того кто прислал, даже если это Ваш друг, знакомый, государственный орган или организация, с которой Вы постоянно ведете переписку, или абсолютно незнакомый человек, прежде чем ее открывать, следует особенно внимательно проверить доменное имя. При возникновении малейшего сомнения, что ссылка ведет не на официальный ресурс, ее необходимо проверить. Сделать это можно отыскав в интернете официальный сайт и сверив домен, либо проверив информацию о дате регистрации домена (у фишинговых обычно от нескольких дней до нескольких месяцев) на интернет-ресурсе https://hb.by/whois.aspx или подобные ему (например: https://whois.net, https://whois.domaintools.com) в поле

«CreationDate».

Если стали жертвой мошенников:

Если ввели данные банковской карты, то необходимо в срочном порядке произвести ее блокировку, позвонив в банк либо, в интернет-банкинге 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.

Статья 349. Несанкционированный доступ к компьютерной информации

Ответственность за деяния, предусмотренные ст.ст. 349-355, наступает с 16-летнего возраста.

Например – несанкционированный доступ (открытие и просмотр файлов, писем, переписки личных данных пользователя и т.п., в нарушение установленного законодательством порядка) к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

Статья 350. Модификация компьютерной информации

В качестве примера можно привести произведенные изменения компьютерной информации в системе либо сети, которые затрудняют либо исключают ее дальнейшее использование.

Статья 351. Компьютерный саботаж

Здесь мы говорим об умышленном уничтожении (удалении, приведении в непригодное состояние, шифровании) компьютерной информации либо ее блокировании (например, путем смены пароля доступа, изменении графического ключа и т.д.).

Статья 352. Неправомерное завладение компьютерной информацией

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации (в обязательном порядке не находящейся в открытом доступе, т.е. защищенной паролем, либо содержание логинов и пароле от учетных записей полученные путем их «взлома»), повлекшие причинение существенного вреда. К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими

лицами.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов. Примером может служить изготовление и сбыт средств (смарт-карт, чипов и т.п.) для неправомерного просмотра зашифрованных телевизионных каналов.

Статья 354. Разработка, использование либо распространение вредоносных программ

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

Указанная статья может быть применена к лицам, имеющим доступ к компьютерным сетям (в том числе к абонентам интернет-провайдеров) и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем либо нарушению правил их использования.

Необходимо отметить, что преступность в сфере противодействия киберпреступности характеризуется высокой степенью латентности, в результате чего реальное количество киберинцидентов существенно выше.

В 2020 году на территории Гомельской области наблюдалась отчетливая тенденция роста количества фактов совершения противоправных деяний в сети Интернет, которые выражались с одной стороны в совершении хищений с карт-счетов граждан путем использования компьютерной техники, с использованием таких видов мошенничеств, как «вишинг» и «фишинг», с другой стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях. Во всех случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению

безопасного использования сети Интернет.

Преступник получает несанкционированный доступ к средству связи с потенциальным потерпевшим, обычно это учетные записи в социальных сетях ВКонтакте, Одноклассники, электронные почтовые ящики, аккаунты в различных программах, предназначенных для обмена сообщениями, например Skype. Чаще всего это становится возможным ввиду небрежного отношение владельца сайта к обеспечению сохранности конфиденциальной информации (логинов, паролей) о пользователях либо беспечности самих пользователей. При этом такая беспечность со стороны пользователей может проявляться в:

попадании на удочку лиц, создавших «фишинговый» (имитирующий настоящий) сайт;

вводе логинов и паролей от своих учетных записей в социальной сети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах;

использовании идентичных реквизитов для авторизации на различных ресурсах;

использовании слишком легких паролей;

установке непроверенного программного обеспечения, предлагаемого на различных сайтах, в том числе, когда такие приложения требуют ввод платежных реквизитов, учетных данных электронной почты или аккаунта в социальной сети;

отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ и др.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы и осуществляет рассылку контактам владельца взломанной учетной записи сообщений мошеннического характера.

Далее преступнику остается ждать отклика от ничего не подозревающих собеседников и проявлять свои способности в риторике и убеждении.

Учитывая изложенные выше факты, приведем некоторые рекомендации для пользователей сети интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

ЗАЩИТА ОНЛАЙН-БАНКИНГА

Необходимо:

Хранить в тайне пин-код карты и другие банковские карты

Прикрывать ладонью клавиатуру при вводе пин-кода

Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы

Использовать лимиты на максимальные суммы онлайн-операций

Скрыть CCV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

Не рекомендуется:

Хранить пин-код вместе с карточкой/на карточке

Сообщать CVV-код или отправлять его фото

Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона) «логин» и «пароль» доступа к системе «Интернет-банкинг»

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.

НАДЕЖНЫЕ ПАРОЛИ

Необходимо:

Создавать персональные (уникальные) пароли к разным сервисам

Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы

Доверять только проверенным менеджерам паролей

Не рекомендуется:

Использовать повторения символов

Хранить пароли на бумажных носителях

Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)

Сохранять пароли автоматически в браузере

Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI

Необходимо:

Отключить общий доступ к своей WI-FI точке, даже если у вас «безлимитный» Интернет, и использовать надежный пароль к ней

Обновить прошивку роутера и сменить пароль к административной панели

Запретить автоматическое подключение своих устройств к открытым WI-FI точкам

Не рекомендуется:

Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам WI-FI в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

Необходимо:

Обновлять браузеры и плагины

Использовать VPN

Не рекомендуется:

Переходить по непроверенным ссылкам

Вводить информацию на сайтах, если соединение не защищено

Сохранять персональные данные в браузере

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

Необходимо:

Подключить двухфакторную аутентификацию

Использовать разную почту для переписок и для регистрации на сайтах

Использовать СПАМ-фильтры

Не рекомендуется:

Реагировать на письма от неизвестного отправителя – скорее всего это спам или мошенники

Открывать подозрительное вложение к письму – сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ

Необходимо:

Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников

Обращать внимание, к каким функциям устройства приложение запрашивает доступ

Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

Не рекомендуется:

Размещать персональную и контактную информацию о себе в открытом доступе

Указывать геолокации на фото в постах

Отвечать на обидные выражения и агрессию в социальных сетях – лучше напишите об этом администратору ресурса

Употреблять ненормативную лексику при общении

Устанавливать приложения с низким рейтингом и отрицательными отзывами.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, **но в общем можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к происходящему в сети Интернет.**

В случае совершения в отношении Вас противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства либо обнаружения факта совершения преступления.

Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!