Информационные материалы об актуальных способах киберпреступлений и мошенничеств, совершаемых с использованием ИКТ для выступления в рамках проведения воспитательно-профилактической работы с гражданами

Фишинг (продажа товаров на интернет-площадках)

Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям и иной персональной информации.

Вы размещаете объявление о продаже товара на торговой площадке, после чего мошенник в мессенджере представляется потенциальным покупателем товара и предлагает осуществить оплату посредством перевода денежных средств на Вашу банковскую платёжную карту, а также предлагает воспользоваться услугами доставки.

При общении мошенник может пояснить, что для осуществления перевода денежных средств на Вашей банковской платежной карточке должна находится сумма равная переводу, в случае если на Вашей банковской платежной карте нет данной суммы мошенник предложит Вам пополнить баланс, все это делается для того, чтобы похитить как можно большую сумму денежных средств.

В случае Вашего согласия на такой способ оплаты мошенник предоставляет ссылку, перейдя по которой Вам предложено ввести реквизиты своей банковской платежной карточки (полный номер карты, срок ее действия, CVV или CVC-код), в случае ввода указанных реквизитов, Вам на мобильный телефон поступает смс-уведомление с кодом подтверждения, после чего на сайте Вам будет предложено ввести поступивший код подтверждения, тем самым Вы подтверждаете перевод денежных средств со своей банковской платежной карты на контролируемые мошенниками банковские счета.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

- вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);

- ведя общение с пользователем стоит перейти на его профиль и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);

- следует воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, в пользу организаций и физических лиц при отсутствии достоверных

данных о том, что названные субъекты являются теми, за кого себя выдают;

- избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить доменное имя (адрес ресурса). Сделать это можно, отыскав в интернете официальный сайт и сверив написание доменного имени. Отличие в одну букву или символ свидетельствует о том, что перед Вами ссылка на поддельный ресурс.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

Фишинг (оплата коммунальных услуг)

В интернет-браузере Вы вводите в поисковой строке «оплата коммунальных услуг, после чего Вам предложены варианты ссылок, перейдя по первой предложенной ссылке вы переходите на сайт внешне схожий с сайтом интернет-банкинга. Для входа в свой личный кабинет Вам предлагается ввести логин и пароль. После ввода указанных данных, Вам на мобильный телефон поступит сеансовый ключ, который также будет предложено ввести на сайте. После ввода сеансового ключа, страница сайта зависает. В этот момент мошенники уже получили доступ к Вашему личному кабинету и совершают хищение денежных средств, имеющихся на Вашем банковском счете.

Советы, как не стать жертвой фишера.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

- очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;

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

Фишинг (покупка билетов в театр или кино)

Молодой человек знакомится с девушкой в интернете. Пообщавшись некоторое время в мессенджере, девушка предлагает ему встретиться в реальности, для первого свидания выбрав поход в театр. Молодого человека не удивляет, что билеты девушка предлагает купить не в театре и не через популярные сервисы для онлайн-бронирования, а на сайте, ссылку на который она сбрасывает.

Парень переходит по ссылке на сайт, который внешне схож с официальным сайтом театра города, в котором проживает молодой человек, после чего заполняет форму для оплаты, где указывает данные своей банковской платежной карты, а также код подтверждения, поступивший ему на мобильный телефон, в дальнейшем у него похищаются денежные средства.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

- внимательно относитесь к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком. Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;

- используйте отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;

- избегайте перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если вам прислали такую ссылку, прежде чем по ней перейти, внимательно проверьте доменное имя (адрес ресурса). Сделать это можно, отыскав в интернете официальный сайт и сверив написание доменного имени;

- отличие в одну букву или символ свидетельствует о том, что перед вами ссылка на поддельный ресурс.

Вишинг

Вам звонит незнакомец. Звонящий представляется работником контакт-центра или службы безопасности банка, также может представится сотрудником МВД Республики Беларусь.

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя». При этом мошенник может знать Ваше имя, а также первые или последние 6 цифр Вашей банковской платежной карточки. После чего мошенник всячески пытается узнать полные реквизиты Вашей банковской платежной карты, Ваши паспортные данные, также мошенник может попросить Вас установить такие приложения как «AnyDesk» или «RustDesk» (данные приложения дают возможность мошенникам удаленно управлять Вашим мобильным устройством), якобы для защиты мобильного приложения банка, которым Вы пользуетесь.

Звонивший сообщает, что разговор записывается и о данном разговоре никто не должен знать, в противном случае Вы будете привлечены к уголовной ответственности.

Все это делается для того, чтобы запугать человека и не дать совершить действия вне инструкции мошенника.

Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

Сотрудники банковских учреждений, а также сотрудники милиции не осуществляют звонки посредством мессенджеров.

Вишинг

(Мошенничество при звонке на домашний телефон)

Отдельного внимания заслуживают случаи мошенничеств под предлогом оказания помощи родственникам, которые якобы стали виновниками совершения дорожно-транспортного происшествия, и для возмещения ущерба либо не привлечения их к ответственности необходимо передать крупную сумму денег.

В ходе общения человека убеждают в том, что он разговаривает со своим близким родственником. После подключается «представитель правоохранительных органов», как правило, «следователь», который уточняет данные и адрес потерпевшего, номер мобильного телефона, он просит не прерывать телефонный звонок. В ходе разговора потерпевшего убеждают передать деньги «помощнику следователя», «адвокату». Курьер получает уточненный адрес, выезжает за деньгами. Все это время, вплоть до получения подтверждения от курьера о получении денег, потерпевший остается на связи с преступниками.

В большинстве случаев потерпевшими становятся граждане пожилого возраста.

В преступную схему в качестве курьеров вовлекаются молодые люди. Они находят сомнительную подработку в одном из мессенджеров.

Юношам и девушкам злоумышленники предлагают забирать денежные средства у одного лица и передать другому, а за это получать 5-15% от суммы денег, которые передавались.

Все курьеры являются наиболее уязвимым местом преступной организации, остальные участники максимально обезличены. После задержания они, как правило, оказывают содействие правоохранителям, при этом их осведомленность не распространяется дальше имени (никнейма) вербовщика и куратора в мессенджере.

В случае поступления звонка от имени работника правоохранительных органов о том, что близкий родственник или знакомые попали в дорожно-транспортное происшествие и им для решения вопроса о не привлечении к ответственности и оказания помощи необходимо передать какие-либо денежные средства, вам необходимо незамедлительно прекратить разговор и связаться с данным родственником. Сотрудники правоохранительных органов никогда не

звонят и не просят передать деньги для оказания помощи в таких ситуациях.

Не поддавайтесь панике, будьте бдительны. Для того чтобы обезопасить себя, своих близких и знакомых от таких противоправных действий проинформируйте их о ставших вам известных способах обманов.

Помните, что наиболее уязвимы перед злоумышленниками пожилые люди, поэтому чтобы уберечь их от беды, на время заберите крупные суммы денег, а также ежедневно напоминайте об опасности.

Незаконный оборот средств платежа

Большое количество граждан по просьбе знакомых или за денежное вознаграждение открывают на свое имя счета в банках. Оформляя банковские платежные карты, пользоваться которыми не собираются, и в нарушение условий договора с банком передают реквизиты третьим лицам. Злоумышленники используют переданные в их пользование карты для перевода, легализации и обналичивания денежных средств, которые получили в результате преступной деятельности. Тем самым человек, который открыл на свое имя банковскую платёжную карту становится соучастником преступления.

Для открытия банковского счета зачастую даже не требуется приходить в банк — все можно сделать онлайн. Особое беспокойство вызывает то, что в эту преступную схему вовлекают подростков в возрасте от 16 до 18 лет, которые даже не осознают противоправности своих действий. С использованием мобильных приложений различных банков они открывают счета, регистрируют электронные кошельки, а затем сообщают злоумышленникам все данные и реквизиты.

Зачастую подростки, получив вознаграждение, по просьбе мошенников подыскивают среди своих друзей тех, кто согласится оказать такую же «услугу», получая за это дополнительную плату.

За изготовление с целью сбыта или сбыт банковских платёжных карт, а также за совершённое из корыстных побуждений незаконное распространение реквизитов карт либо аутентификационных данных лишением свободы на срок до шести лет.

Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, наказываются лишением свободы на срок до десяти лет.

Мошенничества на криптобиржах

С массовым внедрением криптовалют в финансовую систему возросло количество мошенничеств, связанных с криптобиржами. Киберпреступники стали все более изощренными в использовании новых технологий для выявления уязвимостей и мошеннических схем.

В социальных сетях, все чаще можно заметить рекламу сверхвыгодных инвестиционных проектов.

Как только начинающий инвестор клюет на «приманку», его направляют на сайт-опросник от «известного банка» или на красочные сайты одностраничники инвестпроекта. Чаще всего мошенники предлагают желающим быстро разбогатеть вкладываться в криптовалюты или покупку акций известных компаний. Практически каждый из проектов обещает фантастические заработки — от 4000 до 100 тысяч долларов в месяц. Задача мошенника — заставить жертву поверить в инвестпроект, чтоб та оставила свои контактные данные для связи с куратором. После заполнения анкеты, где жертва указывает свои контактные данные, зачастую в мессенджере «Телеграм» с ним связывается тот самый куратор, который будет вести его по ходу всего проекта.

Рассказав в ходе беседы про уникальный проект, где якобы специальная программа помогает зарабатывать деньги на торгах, куратор предлагает пользователю зарегистрироваться в системе и внести депозит, в основном это от 200 до 300 долларов. Если клиент сомневается, ему могут посоветовать забронировать место в проекте, внеся аванс, например, в размере 100 долларов через популярный обменник криптовалют. При подключении к системе в «личном кабинете» будущему инвестору демонстрируют успешные результаты торговли, рост его сбережений, но за красивыми цифрами скрывается пустота — все эти инвестпроекты не предполагают вывод денежных средств, только зачисление.

В ряде случаев менеджер просит сообщить данные банковской карты (включая секретные коды, поступающие на мобильный телефон), с помощью которой потенциальный «участник» планирует делать инвестиции, и якобы отправляет запрос в банк на одобрение внесения депозита. На самом деле деньги просто списываются со счета.

При зачислении первой суммы на биржу, программа якобы начинает свою деятельность по зарабатыванию денежных средств, однако никакой программы нет, а мошенники просто рисуют красивые цифры, которые желает увидеть их клиент. В связи с чем в большинстве случаев жертва не останавливается одним зачислением денежных средств на свой личный кабинет биржи. Жертва может на протяжении нескольких месяцев вкладывать свои кровно заработанные деньги в несуществующий проект, прежде чем поймет, что попался на удочку мошенников.

Не стоит терять бдительность и доверять обещаниям о легком заработке в сети. Преступные схемы совершенствуются каждый день и перед тем, как согласится инвестировать свои накопления, тщательно проверяйте сведения о выбранном интернет-ресурсе.

Мошенничества с розыгрышами бесплатных призов и денежных средств

В различных мессенджерах в основном таких как «Вайбер» неизвестные стали рассылать ссылки с приглашением поучаствовать в различных розыгрышах и получить бесплатные призы или даже денежные средства. Например, мошенники предлагают принять участия в розыгрышах, проводимых "Белпочтой" или каким-либо оператором сотовой связи.

Якобы от имени РУП «Белпочта» мошенники рассылают сообщения в мессенджерах о розыгрыше и предлагают пройти опрос, за который пользователь якобы получит денежную сумму в размере 1000 белорусских рублей. Обращаем ваше внимание, что РУП «Белпочта» не рассылает подобные сообщения и не проводит подобных розыгрышей. Напоминаем, что ни в коем случае не нужно переходить по неизвестным ссылкам, даже если они были предоставлены вашими близкими родственниками и вводить реквизиты своих банковских платежных карт, анкетные данные, в том числе используемые абонентские номера.

Внимательно изучайте адреса сайтов, на которые переходите. Зачастую мошенники регистрируют похожие домены, как у известных организаций. Заменяют, например .by на .cn или просто любую букву в адресной строке.

Мошенничество в сети Инстаграм

Люди знают о том, что многие владельцы аккаунтов в Инстаграм накручивают себе просмотры и подписчиков, создают "липовые" истории, но почему-то забывают, что мошенники тоже умеют это делать.

Разберем на конкретном примере, аккаунт по продаже одежды. В ходе просмотра аккаунта он не вызывает каких-либо подозрений. Хорошее описание, большое количество подписчиков, актуальные истории содержащие отзывы и обзоры продаваемого товара.

Разберем признаки, указывающие на то что данный аккаунт, является мошенническим.

Если обратить внимание на описание мошеннического аккаунта, то мы не найдем здесь никакой информации об офлайн-магазине, куда физически можно приехать и пощупать товар. Также каждый уважающий себя магазин имеет свой сайт, который также всегда указан в описании. На сайте зачастую имеется информация о юридическом адресе и контактных телефонах организации.

Стоит обратить внимание на первую размещенную публикацию на аккаунте. Если первая публикация размещена несколько недель назад, но при просмотре информацию об аккаунте путем нажатия на его имя, мы обнаружим, что аккаунт создан уже несколько лет назад, то данный факт должен вызвать подозрения. Также при осмотре дальнейшей информации необходимо обратить внимание на местоположение аккаунта, на мошеннических аккаунтах оно как правило отсутствует.

В тоже время следует обратить внимание, на раздел «Отметки», если там абсолютно пусто, данный факт указывает на то, что реальные покупатели ни разу не отметили данный магазин у себя в публикациях, несмотря на то, что аккаунт имеет большое количество подписчиков.

Одним из более явных факторов того, что магазин является мошенническим то, что при просмотре публикаций магазина мы не найдем ни одного комментария, а также то, что комментарии к публикациям вовсе ограничены.

В ходе общения администратор аккаунта сообщает вам, что оплата производится только посредством банковской платежной карты, в тоже время предоставляет ссылку якобы для оплаты товара, где будет предложено ввести реквизиты банковской платежной карты, при таком развитии событий необходимо сразу завершить переписку, т.к. в ходе дальнейшего общения администратор всячески попытается оправдать данный способ оплаты и найти множество причин, в связи с чем оплата производится только в таком порядке.

Также в ходе общения вы можете уточнить, имеются ли у магазина офлайн-точки, где можно физически ознакомится с товаром, узнать у продавца контактные данные или юридический адрес организации. Зачастую после перечня данных вопросов администратор, который ведет с вами переписку перестает отвечать на сообщения.

Особенно следует обратить внимание, что пик активности кибермошенников приходится на предпраздничные дни. Для них это самое прибыльное время: десятки людей просматривают сайты в поисках нужных подарков.

Обходите стороной предложения в Инстаграм о продаже товаров по "самым привлекательным ценам", не верьте броским заявлениям, что это якобы "секретная распродажа" или "эксклюзивные поставки прямиком от производителя", не вводите конфиденциальные данные на подозрительных сайтах.

Людей и вправду всегда интересуют товары по низкой цене или акционные предложения. Но не ведитесь на эту удочку в Инстаграм, где мошенники вовсю пытаются сыграть на ваших чувствах и желании сэкономить.

Звонки со стороны «службы поддержки» сотового оператора

Злоумышленники представляются сотрудниками технической поддержки сотового оператора связи и под различными предлогами (продление срока действия сим-карты, несвоевременная оплата счета, случайная блокировка абонентского номера технической службой, сбой в работе оборудования) предлагают абоненту либо перевести деньги на указанный ими номер, либо оплатить штраф, либо перезвонить на короткий номер для решения возникшей проблемы или на номер

телефона, на котором будет включен автоответчик с «рекомендацией», какие действия предпринять абоненту в дальнейшем.

Следует отметить, что злоумышленники могут потребовать жертву установить неизвестные приложения, указать свои паспортные данные, перейти по ссылке или, наоборот, пугают пользователей тем, что их паспортными данными уже якобы кто-то завладел и оформил рассрочку или кредит.

Мошенники используют следующие манипуляции:

«Необходимость обновить приложение мобильного оператора» - это делается для того, чтобы побудить скачать вредоносное программное обеспечение или приложение для удаленного доступа к вашему телефону (по ссылке, в том числе в мессенджере), что позволит злоумышленникам получить доступ к данным, хранящимся в телефоне (личные данные, логины, пароли доступов к банковским приложениям);

«Проведение опроса удовлетворенности работой оператора, ответьте на вопросы, наберите ряд символов на клавиатуре, введите предоставленный пароль» - такая просьба от злоумышленников позволит получить удаленный доступ к системам самообслуживания;

«Срочно, важно, быстро, немедленно, оперативно» - такими словами вас подталкивают выполнить требования мошенников, создав иллюзию ограниченности времени для принятия решений.

Что важно знать:

Сотрудники мобильных операторов не звонят абонентам с использованием мессенджеров, не используют номера иностранных операторов, не требуют изменить пароли под диктовку;

Уточнение персональных данных никогда не происходит по телефону (например, с помощью фото паспорта) и может быть произведено только при личном посещении офисов мобильного оператора;

Чтобы исключить данный вид мошенничества, необходимо помнить, что операторы сотовой связи всегда приглашают абонента в фирменный центр продаж своих услуг в целях решения всех возникших проблемных вопросов.