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.

Вишинг

Вам звонит незнакомец. Звонящий представляется работником различных организаций (МТС, Белтелеком, Водоканал, БрестЭнерго, БелПочта, Домофонный Сервис и т.д.) в ходе разговора звонящий под различными предлогами (продление договора, замена счетчиков/домофонов, получение почтовых отправлений) убеждает Вас в необходимости сообщить свои паспортные данные или данные из смс-сообщений, которые поступят на Ваше мобильное устройство. После сообщения необходимых злоумышленнику данных разговор прекращается.

Далее поступает звонок от имени сотрудников правоохранительных органов или службы безопасности банка. 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 различные приложения по предоставленной им ссылке (данные приложения дают возможность мошенникам удаленно управлять Вашим мобильным устройством), якобы для защиты мобильного приложения банка, которым Вы пользуетесь. Также звонивший под различными предлогами (декларирование денежных средств, погашение кредита) может Вас убеждать осуществить перевод имеющихся денежных средств на указанный им счет.

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.

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.

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.

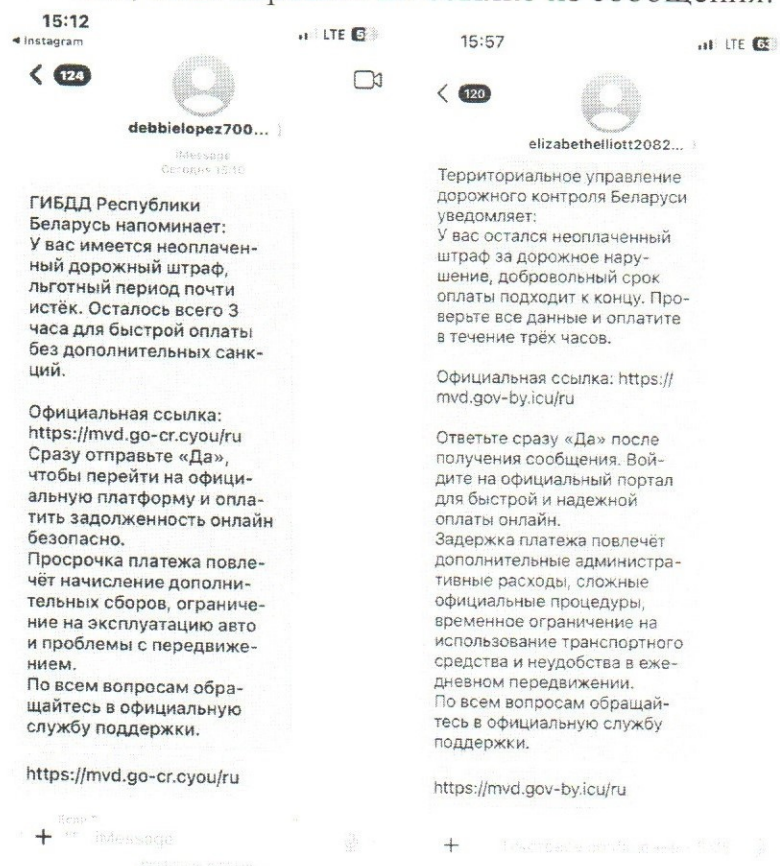
«Ловушка для водителей: штраф в СМС»

Гражданам поступают СМС на мобильные телефоны или сообщения через мессенджеры с уведомлениями о якобы имеющейся задолженности в ГАИ. Для придания легитимности своим действиям преступники используют государственную символику и атрибутику ведомства.

МВД не использует мессенджеры для уведомления о штрафах и не рассылает сторонние платежные ссылки. Официальные интернет-ресурсы органов и учреждений Республики Беларусь расположены исключительно в национальном сегменте сети Интернет – в доменной зоне .by (****./by). Проверка наличия штрафа (задолженности) по линии ГАИ осуществляется только через личный кабинет на сайте МВД (mvd.gov.by), в системе расчетов ЕРИП или непосредственно в подразделениях ГАИ, а оплата штрафов – через ЕРИП и официальные банковские приложения.

Переходя по ссылке, вы попадаете на поддельный сайт (похож на сайт МВД). Введя данные карты, вы переводите деньги мошенникам. Более того, злоумышленники получают данные вашей банковской карты и похищают все имеющиеся деньги.

Никогда не вводите номер банковской карты, срок действия и CVV/CVC-код на сайтах, если перешли по ссылке из сообщения.



Примеры мошеннических сообщений