Актуальные виды киберпреступлений и способы защиты от них.

В настоящее время интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. С одной стороны, это открывает перед белорусскими гражданами и обществом ряд перспектив, с другой – влечет появление новых рисков и угроз.

Так, бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений.

В Гомельской области (как и на территории всей республики) проводится обширная работа по профилактике киберпреступлений, Однако, несмотря на предпринимаемые меры на протяжении нескольких последних лет на территории Гомельской области наблюдается рост количества зарегистрированных киберпреступлений.

НАИБОЛЕЕ АКТУАЛЬНЫЕ ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ:

Фишинг

Отправка поддельных электронных сообщений, текстовых сообщений или создание фейковых веб-сайтов, которые имитируют легитимные коммуникации и требуют у пользователя личные данные — пароли, номера БПК или доступ к учетным записям. Классический пример фишинга — вредоносные ссылки. Например, на фальшивую страницу входа в систему криптобиржи.

Вишинг

Вишинг относится к социальной инженерии, то есть психологическому манипулированию людьми с целью совершения определенных действий или разглашения конфиденциальной информации

Данный способ выражается в осуществлении звонка 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, КГБ, Следственного комитета) и под вымышленным предлогом (пресечение подозрительной транзакции, повышение уровня безопасности пользования картой, перепроверка паспортных данных владельца банковского счета, участия в специальной операции и т. д.) выясняет у потерпевшего сведения о наличии банковских платежных карточек, сроках их действия, CVV-кодах (трехзначный код на обратной стороне

карты), паспортных данных, SMS-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые анкетные данные лиц, на имя которых они выпущены, что позволяет войти в доверие к жертве. В большинстве случаев при совершении звонков преступники используют IP-телефонию.

Покупка товаров через интернет-магазины с предоплатой.

Наиболее примитивной, но от этого не менее работающей формой интернет-мошенничества является размещение преступниками на виртуальных досках объявлений, тематических сайтах, в социальных сетях, группах интернет-мессенджеров объявлений о продаже каких-либо товаров по «бросовым» ценам. Однако для получения товара (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту или электронный кошелек. Правда, после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

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.

Смена домофонного кода

Мошенничество под предлогом обновления домофонного кода – это новый и активно набирающий обороты в республике тип мошенничества

Жертвой такой схемы стала 31-летняя жительница республики.

Правоохранителям пенсионерка сообщила, что в мессенджере ей позвонил неизвестный и представился сотрудником официальной организации по обслуживанию домофонов. Он сообщил, что в доме будет произведена замена кодов домофона и ей в СМС придет два новых кода. Один из которых женщина должна выбрать для дальнейшего использования и сообщить «лжесотруднику». Диктуя код, она и не догадывалась, что на самом деле СМС поступило от банка.

В дальнейшем потерпевшей в мессенджере поступил звонок от якобы правоохранителя, который сообщил, что предыдущий разговор был с мошенником и теперь он завладел её данными, оформил кредит на

её имя, в связи с чем женщине нужно собрать все свои сбережения и положить их в банке на вновь открытый счет.

В данном случае сумма ущерба составила 27 000 рублей.

Незаконные операции с криптовалютой.

Зачастую можно увидеть в социальных сетях, на Ютубе рекламу, призывающую легко заработать. Зачастую, это предложение заработать посредством обмена криптовалюты.

Какие действия с криптой разрешены физлицам в Беларуси?

Согласно Декрету №8 «О развитии цифровой экономики», физические лица вправе владеть цифровыми знаками (токенами, криптовалютой). Отрасль освобождена от налогов до 2049 г., а граждане страны могут не только владеть цифровыми деньгами, но и совершать с ними различные операции:

Майнинг криптовалют.

Хранение криптовалюты в виртуальных кошельках.

Обмен цифровых знаков (токенов, криптовалюты) на иные цифровые знаки (токены, криптовалюту).

Приобретение цифровых знаков (токенов, криптовалюты), их отчуждение за белорусские рубли, иностранную валюту, электронные деньги.

Дарение и завещание цифровых знаков (токенов, криптовалюты).

Причем все эти операции, если они производятся физическими лицами самостоятельно, без привлечения иных лиц, **не являются предпринимательской деятельностью.** Это прописано в пункте 2 статьи 2.2 Декрета №8. **Токены не подлежат декларированию.**

Данная либерализация привлекла большое внимание к рынку криптовалюты. Многие физические лица стали покупать и продавать ее за средства третьих лиц. Однако «помощь» в покупке и продаже криптовалюты третьим лицам может расцениваться как незаконная предпринимательская деятельность.

Пункт 2.6 Декрета Президента Республики Беларусь № 8 **запрещает оказание содействия иным лицам в совершении или исполнении сделок с криптовалютой**.

То есть, физические лица могут осуществлять операции с криптовалютой исключительно в собственных целях, а это значит, что любое посредничество со стороны физического лица в сфере криптовалют является незаконным.

Кроме того, **17 сентября 2024 года** Президент Беларуси Александр Лукашенко подписал Указ № 367 **"Об обращении цифровых знаков (токенов)"**. Документ принят в целях повышения защищенности граждан

при совершении сделок с цифровыми знаками (токенами), а также исключения возможности вовлечения криптовалюты в мошенническую и другую противоправную деятельность.

Указ предусматривает запрет для физических лиц, в том числе индивидуальных предпринимателей - резидентов ПВТ, на покупку и продажу криптовалюты вне белорусских криптобирж (криптообменников).

Как не стать жертвой киберпреступления?

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.

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

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).

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

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.

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.

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

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).

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

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.

Не размещайте фотографии интимного характера в социальных сетях, в закрытых группах, с ограниченным доступом, задумайтесь, если за эту фотографию может быть стыдно, стоит ли ее где-то хранить.

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

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.

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.

Правил много, но в условиях существования в цифровом пространстве это так же элементарно как чистить зубы, пользоваться расческой и купить в аптеке средства защиты.