Что нужно знать, чтобы не стать жертвой мошенничества?

Сложно найти человека, который в своей жизни не сталкивался бы с мошенничеством, сегодня это весьма распространённое преступление.

Высокотехнологичные устройства стали неотъемлемой частью не только отдельно взятого человека, но и общества в целом. Каждый день человек использует в своей деятельности пластиковые карты, мобильные телефоны, компьютер, интернет-ресурсы. Несмотря на все преимущества, современные технологии не всегда используются во благо. Одновременно с развитием таких устройств появляются соответствующие виды мошенничества, позволяющие обмануть и присвоить денежные средства.

Что считается мошенничеством?

Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Лицо, занимающееся этим, называется мошенник или мошенница. В российском законодательстве за подобные действия предусмотрено наказание по статье 159 УК РФ.

**Виды мошенничества в интернете.**

**Фишинг.** Похищение личных данных. У каждого из нас есть конфиденциальные данные. Пин-коды банковских карт, пароли и прочее. В некоторых случаях мошенники, обладающие вашими данными, смогут украсть ваши деньги. Например, совершить покупку с вашей карты без вашего ведома. В основном для фишинга используют почтовую рассылку, содержащую ссылку на фальшивые сайты. Мошенники присылают смс, письма на почту и представляются сотрудниками банка, информируя о том, что по карте необходимо подтвердить какие-то данные, что это обычная процедура, которая не займёт много времени. Злоумышленники начинают расспрашивать, уточнять информацию, присылать дополнительные пароли на телефон, спрашивать ваши коды доступа.

**Мошенничество через сайты объявлений.**

**Мошенник-продавец.**  Мошенник размещает на сайтах объявлении (Авито, Юла, Циан и т.д.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг, за которые в последующем получает предоплату, тем самым похищая денежные средства.

**Мошенник-покупатель.** Мошенник звонит по объявлению потерпевшего, размещенному на сайте и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения, осуществляет перевод через онлайн сервисы или совершая покупку. Или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк, и в последующем похищая денежные средства.

**Виды мобильного мошенничества.**

**Телефонный вишинг (фишинг по телефону). Э**то вид мошенничества, позволяющий в телефонной беседе заполучить требуемые данные.

Злоумышленники представляются какой-то компанией или организацией, выдают себя за официальное лицо, пытаясь обманным путем заставить жертву предоставить свою персональную информацию. Действий от вас ждут прямо во время телефонного разговора. Мошенники создают ощущение срочности, чтобы вы запаниковали и сделали то, чего они хотят. Вот почему они требуют заплатить или раскрыть данные прямо во время звонка, а не просят выполнить какое-то дополнительное действие позднее (после завершения разговора).

**SMS-фишинг**

При SMS-фишинге, или «смишинге», злоумышленники будут призывать вас к действию с помощью текстовых сообщений.

В таком сообщении может содержаться вредоносная ссылка, перейдя по которой вы загрузите на свое устройство вредоносную или шпионскую программу. Но иногда злоумышленники вынуждают жертву совершить другие действия, например, перезвонить на платный номер, оформить подписку или выдать личные данные.

**Мошенничество с банковскими картами.**

Банковская карта является, чуть ли не универсальным средством в финансовом мире – на нее перечисляют заработную плату, выдают кредиты, ею рассчитываются в точках продаж и интернете.

Существует много способов похищения денег с карточки, рассмотреть которые стоит подробнее.

**Звонок от работников банка по сервисному номеру.** В последнее время мошенники активно проводят махинации с картами Сбербанка. Для этого они используют сервисный номер 900. Жертвы получают СМС с номера 900 о списании денег либо проведении махинации с картой. Через некоторое время раздается звонок, где человек, назвавшись специалистом службы безопасности банковского учреждения, просит от клиента отправить ответное смс, где указать код, либо предоставить конфиденциальную информацию. После отправки сообщения, деньги, равно как и сотрудник Сбербанка, бесследно исчезают.

**Скимминг личных данных с карты.** Скимминг - это тип мошенничества, который предполагает незаконное получение данных платёжной карты с помощью различных считывающих устройств.

Для получения необходимых сведений мошенники используют самые разнообразные устройства, которые называются скиммеры. Как правило, их устанавливают в банкоматы или терминалы незаконным путём. Данное оборудование устроено таким образом, что при контакте с картой на него копируется следующая информация: номер, срок действия, CVV-код, фамилия и имя держателя. Также при помощи различных способов и схем злоумышленники узнают ПИН-код карточки. Завладев этими данными, мошенники изготавливают дубликат пластика и снимают все деньги со счёта.

**Простые правила, как не попасться на уловки мошенников**

- Не сообщайте свои персональные данные банковских карт: срок действия, код безопасности с обратной стороны, смс-коды.

- При получении СМС-сообщения о блокировки карты или списании денежных средств, не перезванивайте по указанному в СМС номеру! Чтобы узнать обо всех операциях, перезвоните по номеру, указанному на вашей банковской карточке, сходите в банк лично и проверьте баланс через банкомат/онлайн-банк.

- Осуществляйте заказ товара через проверенные официальные сайты.

- Не сохраняйте свои данные о карте в браузере.

- Не осуществляйте переводы денежных средств в качестве предоплаты, при покупке товара на интернет-сайтах бесплатных объявлений «Авито.ру», «Юла», «Авто.ру» и т.д.

- Скачивайте мобильные приложения только в официальных магазинах (App Store и Google Play).

- Не переходите по коротким ссылкам вида bit.ly и goo.gl, если не доверяете источнику.

- Осмотрите банкомат перед использованием. Убедитесь, что на клавиатуре и в месте для приема карт нет дополнительных устройств, следов клея и механических повреждений.

- Не используйте банкомат с признаками неисправности: устройство зависает, перезагружается или на экране появляются подозрительные изображения.

- Не используйте банкомат в присутствии подозрительных лиц и не принимайте помощь от незнакомцев.