

Как не стать жертвой мошенничества, используя сеть Интернет

Злоумышленник, с целью хищения Ваших денежных средств, размещает в сети Интернет объявление о продаже какого – либо объекта (телефона, квартиры, машины, т.д.) по заниженной цене и оставляет свои контактные телефоны. Вы, заинтересовавшись объектом продажи, как правило связываетесь с мошенником, он сообщает что для покупки товара необходимо внести предоплату(на расчетный счет, Яндекс- деньги, счет вебмани и т.д. при этом может выслать копию поддельного паспорта для придания Вашей уверенности что обмана нет). Злоумышленник объясняет внесение предоплаты тем что живет в другом регионе и отправит товар сразу же после того как удостовериться в оплате товара. Наиболее частыми площадками для размещения подобных объявлений являются сайты социальных сетей «В контакте», «Instagram», «Одноклассники» , также могут выступать ресурсы бесплатных объявлений «Авито», «Юла», «auto.ru».

Также распространенным способом мошенничества в сети интернет , является создание сайтов интернет – магазинов . Злоумышленник по электронной почте высылает договор , который заполняет заказчик, после чего просит внести предоплату за товар. Также встречается создание сайтов – клонов, на которых искажены реквизиты получателя. Сайты клоны создаются таким образом, что пользовательский интерфейс является копией оригинального Интернет – ресурса. Различие может заключаться только в имени (например, оригинальный ресурс «**tech – point.ru**», а сайт двойник «**tex- point.ru**»). Внимательно читайте названия интернет – магазинов, пробуйте зайти на его сайт с других сайтов, тем самым вы сразу обнаружите сайты – клоны. Не сообщайте при покупке товара сведения с вашей банковской карты. Не заказывайте товар с сомнительных сайтов, где при покупке одного товара, Вам второй идет в подарок, как правило при получении посылки на почте в ней находится товар не соответствующий заявленному .

Как не стать жертвой мошенничества с банковскими картами при использовании услуги «мобильный банк»:

В случае потери мобильного телефона с подключенной услугой «Мобильный банк» или мобильным приложением «Сбербанк Онлайн» следует срочно обратиться к оператору сотовой связи для блокировки сим – карты, и контактный центр банка для блокировки услуги «Мобильный банк» или «Сбербанк Онлайн». Кроме этого при смене номера телефона, на который ранее была подключена услуга «Мобильный банк», необходимо обратиться в любой филиал банка, с целью отключения данной услуги от старого номера и подключения на новый. Не следует оставлять свой телефон без присмотра. Не подключайте к данным услугам абонентские номера, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников банка.

При пользовании банковскими картами , с целью избежания несанкционированных действий с использованием карты, необходимо проведение операций по ней только в вашем присутствии, никогда не позволяйте уносить третьим лицам карту из поля вашего зрения. В случае обращения какого – либо лица лично, по телефону, в сети «Интернет», через социальные сети или другим способом, которое под различным предлогом пытается узнать полные данные о вашей банковской карте (16-ти значный номер, срок действия, данные владельца, трехзначный код проверки подлинности карты, пароль и другую персональную информацию), будьте бдительны – это явные признаки противоправной деятельности. При любых сомнениях необходимо прекратить общение и обратиться в банк по телефону указанному на оборотной стороне карты. Во избежании использования карты другим лицом, следует хранить ПИН- код отдельно от карты, не писать ПИН- код на карте, не сообщать родственникам, не переходить по ссылкам и не устанавливать приложения (обновления пришедшие по SMS/ MMS электронной почте , мессенджерам (Вайбер, Вацап и д.р.) в том числе если они пришли от имени банка. Помните что банк не рассылает своим клиентам ссылки или указания подобным образом.

Если Вам позвонили с поликлиники и сообщили , что у Вашего родственника обнаружен страшный диагноз и на его лечение необходимо перевести деньги за лекарства по указанным реквизитам - прервите разговор – это мошенники. Проверьте информацию,

свяжитесь с родственниками. Медицинские учреждения принимают денежные средства только после заключения соответствующего договора и только в вашем присутствии.

Если вы получили смс – сообщение с незнакомого номера о выигранном призе, но для его получения Вам необходимо пройти по определенной ссылке или с просьбой положить определенную сумму на указанный номер телефона или перевести деньги на счет, или вернуть деньги как ошибочно переведенные Вам – это мошенники .

Не верьте подобным сообщениям, не переходите по ссылкам, не отвечайте на сообщения, не пользуйтесь услугами сомнительных интернет – магазинов, будьте бдительны и берегите себя

ОМВД России по Нерчинскому району