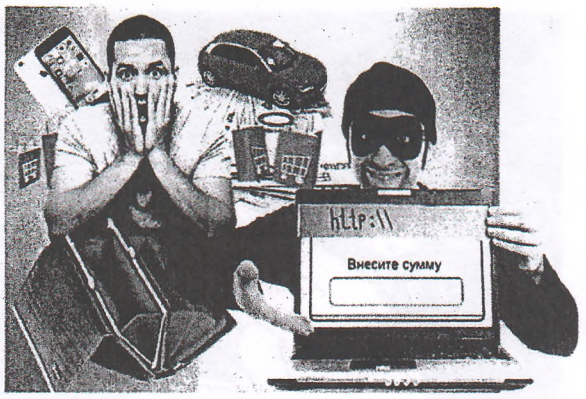
Злоумышленник, с целью хищения Ваших денежных средств, размещает в сети Интернет объявление о продаже какого-либо объекта (телефон, машина, квартира) по заниженной цене и оставляет свои контактные данные.

После того, как Вы собираетесь приобрести товар, связываетесь с мошенником, он сообщает, что для покупки необходимо внести предоплату (на расчетный счет, счет, яндекс - деньги, счет вебмани и т.д.).

Наиболее часто встречающимися площадками для размещения подобных объявлений является сайты социальных сетей **«В контакте», «Instagram», «Одноклассники»,** также такими сайтами могут выступать ресурсы бесплатных объявлений **«Авито», «Юла» и «auto.ru».** Злоумышленник объясняет внесение предоплаты тем, что живет в другом регионе и отправит товар сразу после того, как удостовериться уплате за товар. Злоумышленник может выслать копию паспорта (поддельную).

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 доменном имени (например оригинальный ресурс «tech-point.ru» и сайт двойник «tex-point.ru»).



- Интернет-магазины с хорошей репутацией работают без предоплаты, товар на дом привозит курьер, только после осмотра и проверки товара продавец платит деньги;

- прежде чем заказать товар в Интернете, почитайте отзывы на разных сайтах о данном Интернет-магазине или виртуальном продавце, как правило, Вы сразу обнаружите отрицательные отзывы либо их отсутствие о выбранном Вами Интернет-магазине (следует сделать вывод о коротком периоде его существования),:

- внимательно читайте названия Интернет-магазина, пробуйте зайти на его сайт с других сайтов, тем самым Вы сразу обнаружите сайты-клоны;

- избегайте покупки товара по предоплате;

- если цена товара гораздо ниже цены как в обычных розничных магазинах, так и в других Интернет-магазинах, либо на рынке в целом (например, при продаже автомашины по заниженной стоимости), задумайтесь!;

- запрос покупателем, якобы для перечисления предоплаты, либо оплаты за товар информации не только о шестнадцатизначном номере карты (требуется исключительно только он), сроке ее действия, данных владельца и трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты также является одной из схем действия мошенников. Не сообщайте при покупке товара сведения о Вашей банковской карте.

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 SIM-карты и в Контактный центр Банка для блокировки услуги «Мобильный банк» и/или «Сбербанк Онлайн».

При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение), с целью отключения услуги «Мобильный банк» от старого номера и подключения на новый.

Не следует оставлять свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг другими лицами.

Не подключайте к услуге «Мобильный банк» 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 избежать несанкционированных действий с использованием карты, необходимо требовать проведения операций с ней только в Вашем присутствии, никогда не позволять уносить третьим лицам карту из поля Вашего зрения.

В случае обращения кого-либо лица лично, по телефону, в сети «Интернет», через социальные сети или другим способом, которое под различными предлогами пытается узнать полные данные о вашей банковской карте: шестнадцатизначном номере, сроке действия, данных владельца, трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты и т.д. (паролях или другой персональной информации), **будьте осторожны - это явные признаки противоправной деятельности.** При любых сомнениях рекомендуется прекратить общение и обратиться в банк по телефону, указанному на обратной стороне банковской карты.

Не следует прислушиваться к советам третьих лиц, а также отказаться от их помощи при проведении операций. В случае необходимости, обращаться к сотрудникам филиала банка или позвонить по телефонам, указанным на устройстве или на обратной стороне карты.

Во избежание использования карты другим лицом, следует хранить ПИН-код отдельно от карты, не писать ПИН-код на карте, не сообщать ПИН-код другим лицам (в том числе родственникам).

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие поSMS/MMS/электронной почте/мессенджерам (Вайбер, ВацАп и др.), в том числе от имени Банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.