**МВД ИНФОРМИРУЕТ!**

**Внимание.** Отмечается распространение нового способа дистанционного мошенничества, где злоумышленники, для своей маскировки все чаще используют (Интернет)-телефонию с подменой абонентского номера звонящего (8-800,8-495,8-499 и т.д.) которая позволяет преступнику остаться анонимным. С такой возможностью преступники осуществляют звонки на мобильные телефоны граждан под видом сотрудников банков (с информацией о блокировке банковской карты, о взятии кредита по карте и т.д), часто используют номера реальных банков, финансовых организаций, подразделений МВД и других правоохранительных органов. В ходе совершения преступления, могут представляться сотрудниками МВД, ФСБ прокуратуры и т.д. Могут направлять потерпевшим на мобильные телефоны всевозможные CMC сообщения, справки от банков и правоохранительных органов, а также информацию о подтверждении операций.

**Как себя защитить:**

1. Бдительно относитесь к предупреждениям от операторов сотовой связи, правоохранительных органов и средств массовой информации о схемах обмана.
2. Убеждайтесь в достоверности информации, полученной по телефону от неизвестных. Перезванивайте родственникам и знакомым - лучше прослыть излишне подозрительным, чем быть обманутым.Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученных посредством телефонного звонка, CMC или ММС, якобы, от сотрудников банка, в особенности, если они требуют произвести манипуляции с банковской картой. Не говорите незнакомцам свои ФИО, реквизиты паспорта и другие личные данные. Не оправляйте пустые CMC, либо с набором цифр, которые Вам продиктовали, это может быть служебная команда Интернет-банка на перевод денежных средств с Вашей карты. **Внимание звонок «из банка»**Один из широко известных приемов телефонных мошенников-звонок на мобильный телефон якобы из службы безопасности банка с сообщением о проблеме, сбое или попытке незаконного списания денег с Вашей карты. **Обращаем внимание,** что при звонке клиенту сотрудник банка никогда **не просит конфиденциальные сведения;** полные реквизиты карты (номер карты, ПИН или CVV-код), CMC-пароли банка, логин и пароль для входа в онлайн-банк, контрольную информацию (кодовое слово); никогда не требует совершать каких-либо операций с картой, в том числе брать кредит и деньги перечислять на номера мобильных телефонов, и счета банковских карт. И самое главное: при любых сомнениях, подозрениях или беспокойстве, при малейшей попытке собеседника узнать пароли или коды немедленно завершите разговор. А затем перезвоните по правильному контактному номеру банка, проверив его на сайте банка или на обороте своей карты.Как не стать жертвой мошенничества используя сеть интернет.Злоумышленник, с целью хищения денежных средств, размещает в сети Интернет объявление о продаже какого-либо объекта (телефон, машина, квартира и т.д.) по заниженной цене и отправляет 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 веб мани и т.д.).

Наиболее часто встречающимися площадками для размещения подобных объявлений являются сайты социальных сетей «В контакте», «Instagram», «Одноклассники», также такими сайтами могут выступать ресурсы бесплатных

объявлений «Авито», «Юла» и [«auto.ru»](NULL). Злоумышленник объясняет внесение предоплаты тем, что живет в другом регионе и отправит товар сразу после того, как удостоверится в уплате за товар. Злоумышленник может выслать копию паспорта (поддельную).

Также, распространенным способом мошенничества в сети интернет, является создание сайтов-клонов интернет магазинов, на которых искажены реквизиты получателя. Сайты-клоны создаются, таким образом, что пользовательский интерфейс является копией оригинального Интернет-ресурса. Различие может заключатся только в доменном имени (например, оригинальный ресурс «tech-[point.ru»](http://point.ru), а сайт двойник [«tex-point.ru»](NULL)).

**Надо помнить, что:**

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

-прежде чем заказать товар в интернете, прочитайте отзывы на различных 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 выводы и 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, продавцом/покупателем, якобы для перечисления предоплаты, либо оплаты за товар информации не только о шестизначном номере карты (требуется исключительно только он) но и сроке действия, данных владельца, трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты и т.д. (паролях и другой персональной информации), будьте осторожны - это явные признаки противоправной деятельности. При любых сомнениях рекомендуется прекратить общение.

Не следует прислушиваться к советам неизвестных Вам лиц, а также отказаться от их помощи при проведении операций. В случае необходимости, обращаться к сотрудникам филиала банка или позвонить по телефонам, указанным на оборотной стороне карты, либо на официальном сайте банка.

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 переходить по ссылкам и не устанавливать приложения/обновления, пришедшие по SMS/VVS/электронной почте/мессенджерам (Viber, WatsApp и др.), в том числе от имени банка. Помните, что банк не рассылает своим клиентам ссылки и указания подобным образом.

**Будьте бдительны не дайте себя обмануть.**