**Как не стать жертвой мошенников**

Мошенники оказывают психологическое воздействие на  человека таким образом, чтобы он  раскрыл личные или финансовые данные, перевел им деньги или даже взял кредит для последующей передачи средств в чужие руки. Они могут неоднократно звонить жертве, в том числе используя технологию подмены телефонных номеров, направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых организаций, так и любых других компаний и маркетплейсов. Злоумышленники всячески пытаются вывести человека из спокойного состояния и  отключить у  него логическое мышление. Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться заинтересовать и обрадовать внезапной выгодой. Схемы мошенников часто выглядят очень правдоподобно, так  как  они  используют самые обсуждаемые новости или события.

**Как не стать жертвой мошенников, общие рекомендации:**

1. Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.
2. Если с неизвестного номера звонит якобы сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Самостоятельно позвоните в банк по номеру телефона, указанному на обратной стороне карты или  на  его  сайте, или  в  контакт-центр ведомства, сотрудником которого представлялся звонящий.
3. Не совершайте каких-либо действий по  счету, если вам  звонят с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный счет», например в Центробанке, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.
4. По возможности установите антивирус на все устройства и обновляйте его.
5. Совершайте покупки в Интернете только на проверенных сайтах. Заведите отдельную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).
6. Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

**Если вы стали жертвой мошенников:**

Шаг № 1. Немедленно заблокируйте карту с помощью мобильного приложения или личного кабинета на сайте банка. Заблокировать ее также можно через контакт-центр банка (телефон указан на оборотной стороне карты) или в любом его отделении.

Шаг № 2. В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией. Также обратитесь с заявлением о хищении денег в любое отделение полиции.

**ПОМНИТЕ:** если вы  самостоятельно перевели деньги мошенникам или предоставили им банковские данные, то банк не обязан возвращать похищенную сумму.