

Как не стать жертвой мошенников? Проверенные советы от Центрального банка России.

- 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.
- 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.
- 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.
- По возможности установите антивирус на все устройства и обновляйте его.
- 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).
- 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.

ОСТОРОЖНО: МОШЕННИКИ! НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ




Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) sms-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



СООБЩЕНИЯ ОТ ДРУЗЕЙ



Мошенник пользуется чужой страницей в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ



Сообщение о блокировке банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫГРЫША (компенсация за потерянный вклад)



Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ



Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не переходите по сомнительным ссылкам.

ГРАЖДАНЕ, БУДЬТЕ БДИТЕЛЬНЫ! ЕСЛИ ЖЕРТВАМИ МОШЕННИКОВ СТАТЬ НЕ ХОТИТЕ ВЫ!

**ЗВОНИТ МОБИЛЬНИК, И ГОЛОС ПРИЯТНЫЙ
ВАМ ГОВОРИТ, ЧТО ПРИЗ НЕОБЪЯТНЫЙ
ВЫИГРАН ВАМИ - НЕ ВЕРЬТЕ,
ВЫСЛУШАВ НОВОСТЬ, ПРОВЕРЬТЕ!**

**ЕСЛИ ПРИШЛО SMS НЕПОЯТНОЕ,
В НЕМ СОДЕРЖАНИЕ ВЕСЬМА НЕПРИЯТНОЕ:
СЫНУ ИЛИ ДОЧЕРИ ЧТО-ТО ГРОЗИТ,
ДЕНЬГИ СКОРЕЙ ПОЛОЖИ ИЛИ ВЕЗИ.
СРАЗУ СЛЕЗЫ НЕ ЛЕЙТЕ,
ПЕРЕЗВОНИТЕ, ПРОВЕРЬТЕ!**


