

СТОП МОШЕННИЧЕСТВО

КАК ПРОИСХОДИТ:

Вам позвонил работник банка и сообщил о:

- попытке списания денежных средств с карты;
- переводе средств на чужую банковскую карту;
- поступлении заявки в банк на онлайн-кредит;
- хакерской атаке на личный кабинет банка.

Часто мошенниками используется «подмена номера», т.е. при звонке может быть указан любой номер телефона, в том числе номер банка, государственных структур, правоохранительных органов.



КАК ИЗБЕЖАТЬ:

ПРЕКРАТИТЕ РАЗГОВОР!!!

НЕЛЬЗЯ сообщать свои персональные данные, номера банковских карт, пароли из смс-сообщений и т.д.!

НЕЛЬЗЯ устанавливать на мобильный телефон различные приложения под видом проверки устройства на вирусы!

НЕЛЬЗЯ выполнять требования звонящего следовать к банкомату и проводить действия под его руководством!

НЕЛЬЗЯ привязывать к функции бесконтактной оплаты незнакомые банковские карты!

При любых сомнениях обратитесь в офис банка.

ПОМНИ:

МОШЕННИКИ ОРУДУЮТ ВЕЗДЕ



При изготовлении банковской карты используются передовые технологии в области защиты от действий третьих лиц!

Как правило потерпевшие сами сообщают всю необходимую информацию мошеннику, тем самым облегчая доступ к своему банковскому счету!

Работники банков НИКОГДА не запрашивают реквизиты банковской карты (номер карты, код с обратной стороны карты), пароли из смс-сообщений, и т.д.!

Сотрудники полиции не осуществляют звонков потерпевшим с требованиями оказывать помощь специалистам банка, чтобы вычислить недобросовестного банковского работника!

КАК ПРОИСХОДИТ:

Вы разместили объявление о продаже товара или оказания услуг на сайтах бесплатных объявлений, после чего потенциальный покупатель сообщил, что оплатил товар и прислал ссылку для получения денежных средств.

Вы покупаете товар на сайтах бесплатных объявлений, в Интернет-магазинах, в социальных сетях. Продавец требует заранее оплатить товар, либо прислал ссылку для оплаты товара, при этом убеждает наличием транспортной накладной.



КАК ИЗБЕЖАТЬ:

НИКОГДА не переходите по ссылкам, которые скидывает вам покупатель или продавец.

Если есть необходимость отправить или получить товар, то все сделки проводите через официальный сайт!

ОБЯЗАТЕЛЬНО перепроверьте контактную информацию (ИНН, КПП, ОГРН, банковские реквизиты), размещенную на странице Интернет-ресурса!

ВСЕГДА проверяйте наличие отзывов о работе Интернет-магазина! Отсутствие отзывов — знак для размышлений!

Whois сервисы помогут узнать возраст сайта, его владельца и другую полезную информацию!

ПОМНИ:

Злоумышленники могут использовать страницы, внешне похожие на официальный сайт. Мошенники могут позаимствовать даже логотип и дизайн!

Каждый Интернет-сервис на своем сайте размещает информацию о противодействии мошенничеству. **НЕ ЛЕНИТЕСЬ** ознакомиться с рекомендациями безопасных сделок!

Недобросовестные Интернет-магазины на своем сайте сами публикуют явно поддельные отзывы!

Если вместо удобной формы оплаты вы видите просто номера банковских карт, электронных кошельков, на которые вам предлагают перевести деньги — это значит, что платеж уходит не официальной компании, а физическому лицу!

На сайте транспортной компании всегда можно проверить транспортную накладную, либо наличие отправления на ваше имя!