

Звонки из службы безопасности банка



Вам поступают звонки с номеров, начинающие с «+7495...», где неизвестные лица представляются сотрудниками службы безопасности банка

- сообщают о подозрительных операциях по вашим банковским счетам, несанкционированных списаниях денежных средств
- в отношении вас совершаются мошеннические действия
- ваша карта заблокирована
- предлагают перевести денежные средства на резервные безопасные банковские счета, ячейки
- требуют подойти к ближайшему банкомату и перевести денежные средства на банковские счета или абонентские номера, которые диктуются мошенниками

**НЕ СОВЕРШАЙТЕ НИКАКИХ ОПЕРАЦИЙ ПО ИНСТРУКЦИЯМ ЗВОНЯЩЕГО
СРАЗУ ЗАКАНЧИВАЙТЕ РАЗГОВОР**

**НАСТОЩИЙ РАБОТНИК БАНКА НИКОГДА НЕ БУДЕТ ПОПРОСИТЬ У ВАС
КОДЫ БЕЗОПАСНОСТИ С ОБРАТНОЙ СТОРОНЫ КАРТЫ (CVV/CVC), ЛОГИН
ОТ ОНЛАЙН-БАНКА, КОДЫ ИЗ СМС, НОМЕР БАНКОВСКОЙ КАРТЫ**

Мошенничества в социальных сетях, приложениях на смартфонах и Интернет-сайтах



- В социальных сетях есть «всплывающая» реклама с предложениями дополнительного заработка денег, компенсации за какие-либо услуги, крупный выигрыш, социальные выплаты и заработок на биржевом или валютном рынке, это тоже мошенническая схема, которая в конечном итоге приводят к потере денежных средств.
- Также помните, страницы ваших друзей могут взломать мошенники. Не поддавайтесь на просьбы о займе денежных средств. Убедитесь лично, что вашим друзьям требуется финансовая помощь.
- Никогда не переходите по ссылкам из писем и смс-сообщений от неизвестных отправителей. Участились случаи, в том числе на бла-бла-кар, когда мошенники в мессенджерах требуют перейти по ссылке для совершения оплаты поездок, товаров или услуг.

**НЕ ПЕРЕВОДИТЕ ДЕНЕЖНЫЕ СРЕДСТВА НЕЗНАКОМЫМ ЛИЦАМ НИ ПОД
КАКИМ ПРЕДЛОГОМ**

Мошенничества на сайтах бесплатных объявлений «Авито», «Дром.ру» и т.д.



Мошенничество может быть как со стороны продавца, так и со стороны покупателя

- Не соглашайтесь на предоплату при покупке или продаже товара. Мошенники всегда будут Вас торопить с оплатой товара.
- Перепроверяйте ссылку на Интернет-сайт. Мошенники могут использовать сайты-двойники. В адресной строке браузера должен быть значок в виде закрытого замка. Делайте покупки только на сайтах, которые обеспечивают безопасное соединение.
- Вам могут скидывать скан-копии паспорта, чтобы показать «честность» продавца и присылать поддельные накладные с транспортных компаний. Но помните, что при современном развитии техники, изготовить изображение паспорта или документы на отправку товаров не представляет никакого труда.

ВСЕГДА ПРОЯВЛЯЙТЕ ВНИМАТЕЛЬНОСТЬ ПРИ ОБЩЕНИИ С ПРОДАВЦОМ ИЛИ ПОКУПАТЕЛЕМ. ЕСЛИ ОТ ВАС СРОЧНО ТРЕБУЮТ ДЕНЬГИ, СНЕСТИ ПРЕДОПЛАТУ, ПЕРЕЙТИ ПО ССЫЛКАМ – СДЕЛАЙТЕ ПАУЗУ И ПРОАНАЛИЗИРУЙТЕ СИТУАЦИЮ, ВОЗМОЖНО, ВЫ РАЗГОВАРИВАЕТЕ С МОШЕННИКОМ

Звонки с использованием подменных номеров



Гражданину звонит незнакомец, представляется сотрудником банка и сообщает, что злоумышленники пытаются оформить онлайн-кредит на его имя

- Якобы для того, чтобы предотвратить незаконные действия, человека убеждают в необходимости самостоятельно оформить онлайн-кредит, обналить поступившие на банковскую карту деньги и перечислить их на счет для мгновенного погашения кредита.
- Через несколько минут ему звонит соучастник преступной схемы, который представляется полицейским и рекомендует следовать инструкциям звонивших ранее представителей банка. При этом злоумышленники используют современную технологию подмены данных, которая позволяет имитировать звонок с номеров, указанных на официальных сайтах правоохранительных органов и иных организаций.

ЕСЛИ ВАМ ПОЗВОНИЛИ И ПРЕДСТАВИЛИСЬ СОТРУДНИКАМИ КАКИХ-ЛИБО ОРГАНИЗАЦИЙ – САМОСТОЯТЕЛЬНО ПЕРЕЗВОНИТЕ ПО ОФИЦИАЛЬНЫМ НОМЕРАМ И УТОЧНИТЕ ВСЮ ИНФОРМАЦИЮ