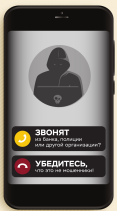


Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА



- НА ВАС ВЫХОДЯТ САМИ**
Аферисты могут предаться службой безопасности банка, налоговой, прокуратурой.
Любой неожиданный звонок, SMS или звонок — повод насторожиться.
- РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ**
Сильные эмоции притупляют бдительность.
- ЗВОНЯТ**
Или пишут сообщения.
- УВЕДИТЬСЯ**
- НА ВАС ДАВЯТ**
Аферисты всегда говорят, чтобы у вас не было времени все обдумать.
- ГОВОРИТ О ДЕНЕГАХ**
Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект.
- ПРОСИТ СООБЩИТЬ ДАННЫЕ**
Злоумышленники интересуют реквизиты карты, пароли и коды из банковских уведомлений.

ВАЖНО!
Сотрудники Банка и полиции **НИКОГДА** не спрашивают реквизиты карты, пароли из SMS, персональные данные и не просят совершать переводы с вашей карты.

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из SMS
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовые слова
- персональные данные

Как защитить свои финансы, читайте на fsccs.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт.

Какие схемы используют аферисты?

- ОБЩАЮТ ЗОЛОТЫЕ ГОРЫ**
Ссылаются на валютные курсы, социальные выплаты или ссудоразрешительные инвестиционные проекты. Трудно быстрое обогащение — признак обмана.
- ЗАМАНИВАЮТ НА РАСТРОДАЖИ**
Отправляют скриншоты и видео, где якобы ведется аукционирование уникальных объектов.
- СПЕКУЛИРУЮТ НА ПРОМЕЖИ СОБЫТИЙ**
Намерены обмануть сбор денег на разработку вакцины, объявляют конкурс, деньги за выполнение работы или призовут получить государственные дотации.
- МАСКИРУЮТСЯ**
Имитируют роль продавца и покупают на популярном сайте объявлений.

Как обезопасить свои деньги в интернете?

- 1 Установите антивирус и регулярно обновляйте его.
- 2 Заведите отдельную дебетовую карту для покупок в интернете и карты не берите чаще трех разов в месяц.
- 3 Всегда проверяйте адрес электронной почты и сайтов — они могут отличаться от официального лишь парой символов.
- 4 Не переходите по ссылкам из мессенджера — сразу удаляйте сомнительные сообщения.
- 5 Никогда не сообщайте свои персональные данные.

Подробнее о вариантах защиты читайте на fsccs.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций.

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылке из интернета или электронной почты, SMS, сообщений в соцсетях или неспециализированной рекламе, объявлений о лотереях, распродажах, компенсациях от государства.

- Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых.

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего лишь парой символов.
- В адресной строке нет HTTPS и значка закрытого замка.
- Далеко спрятан логотип организации, в текстах есть ошибки.
- У сайта мало страниц или даже одна — для ввода данных карты.

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- Установите антивирус и регулярно обновляйте его.
- Сохраняйте в закладках адреса нужных сайтов.
- Не переходите по подозрительным ссылкам.
- Используйте отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой.

Подробнее о вариантах защиты читайте на fsccs.info

Финансовая культура

 Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

- 1 ЗАБЛОКИРОВАТЬ КАРТУ**
 - по номеру телефона Банка на банковской карте или на официальном сайте
 - через мобильное приложение
 - через личный кабинет на официальном сайте Банка
 - в отделении Банка
- 2 НАПИСАТЬ заявление о несогласии с операциями**
 - Заявление должно быть написано
 - в течение суток после сообщения о списании денег
 - на месте в отделении Банка
- 3 ОБРАТИТЬСЯ в полицию**
 - Чем больше людей подаст заявление, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- сроки действия карты и транзакционный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логики и пароли от онлайн-банка

НЕ ПУБЛИКУЙТЕ персональные данные в открытом доступе

УСТАНОВИТЕ антивирус на все устройства

КОДОВОЕ СЛОВО называйте только сотруднику Банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

 Подробнее о правилах безопасности читайте на [kardinfo.ru](#)

 Финансовая культура

 Банк России

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн и мобильного банка
- перевзламывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов

КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Появляются всплывающие окна
- Торчат объемы памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- Позвоните в Банк и попросите заблокировать доступ к онлайн и мобильному банку у всех карт, которые использовали на устройстве
- Обратитесь в сервисный центр, чтобы выслать гаджет
- Перезагрузите карту, смените логики и пароли от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- Используйте антивирус и регулярно его обновляйте
- Не переходите по ссылкам от неизвестных, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения только из проверенных источников
- Обновляйте операционную систему устройства
- Избегайте общественных Wi-Fi-сетей

 Подробнее о защите гаджетов читайте на [kardinfo.ru](#)

 Финансовая культура