



Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА



1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо – повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений



ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты



НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

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



Как защитить свои финансы,
читайте на fincult.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?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ

Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

ЗАМАНИВАЮТ НА РАСПРОДАЖИ

Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ

Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ

Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
- 5 Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на fincult.info

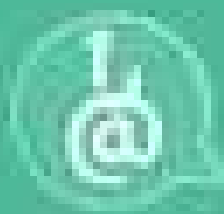


Финансовая культура



КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

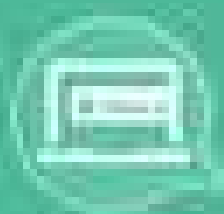
Фишинг – это мошенничество, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций.



КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

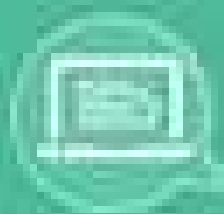
На сайты фишинга можно попасть или через поисковую систему, СМС-сообщения и социальные сети, или по электронной почте, или по объявлению в интернете, или по рекламе, размещенной на сторонних интернет-ресурсах.

Важно не только выбирать надежные ресурсы, но и внимательно читать условия и читать отзывы других людей об интернет-ресурсах.



КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего (или вовсе отсутствует)
- В адресной строке нет слова «https» (или оно выделено другим цветом)
- Дизайн и содержание отличаются от настоящего сайта
- У сайта есть «подпись» или «подпись» отсутствует



КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- Устанавливайте антивирус и регулярно обновляйте его
- Сравнивайте в интернете адреса реальных сайтов
- Не переходите по подозрительным ссылкам
- Рассмотрите возможность установки для браузера и смартфона, смартфона на ваш смартфон функции поиска фишинга

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ



- на сайте или по телефону Банка на Псковской карте или по 800-200-0000 по всей России
- через мобильное приложение через личный кабинет на Псковской карте Банка
- в отделении Банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕДОСТУПНОСТИ СРЕДСТВ



- в отделении Банка
- в личном кабинете клиента
- по почте в отделении Банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



- для подачи заявления о краже денег с карты
- для получения справки

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ

- свои данные карты и личный код
- не выкладывайте сканы документов
- номера и сроки их действия
- карты и сроки их действия

НЕ ПУБЛИКУЙТЕ

персональные данные в интернете для всех

УСТАНОВИТЕ

защиту на все устройства

КОДОВОЕ СЛОВО

не сообщайте никому, включая Банк, номер своего личного кодового слова



Банк не компенсирует потери, если вы нарушите правила безопасности использования карты

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- распространяют вредоносный доступ к вашим устройствам
- крадут логины и пароли от почты и мобильного банка
- перехватывают секретные коды из сообщений

Возможные эти данные, хакеры-преступники могут похитить все данные с ваших счетов



КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАИЖЕНО?

- Появились уведомления или сообщения
- Сильно замедлился процесс загрузки
- Появились приложения, которых нет
- Телефон часто перегревается

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- Переключитесь в режим безопасности (заблокировать доступ к интернету и мобильному банку и все карты, которые использовались на устройстве)
- Обратитесь в сервисный центр, чтобы выслать телефон
- Переинсталируйте карты, удалите логины и пароли от почты, банка и других приложений (включая мессенджеры)

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- Обновляйте операционную систему и приложения на регулярной основе
- Не скачивайте приложения из неизвестных источников, не устанавливайте программы, не из PlayStore и не используйте бумажные файлы
- Скрывайте персональные данные на приватных устройствах
- Обновляйте идентификацию на своем устройстве
- Не используйте общедоступные Wi-Fi сети