



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

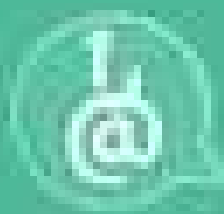


Финансовая культура



КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

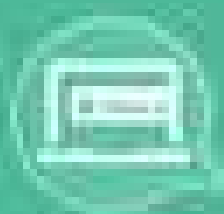
Фишинг – это мошенничество, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций.



КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

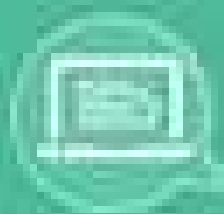
На сайты фишинга можно попасть или через поисковую систему, СМС-сообщения в интернете или рекламные объявления, размещенные в интернете, рекламные рассылки, электронную почту и т.д.

Важно не только выбирать надежные ресурсы, но и внимательно читать письма и сообщения.



КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего (или имеет странное расширение)
- В адресной строке нет слова «https» (или оно выделено другим цветом)
- Дизайн и содержание отличаются от настоящего сайта
- У сайта есть ошибки или странная структура страниц



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 электронной почты на свой компьютер специальной защиты

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ



- на номер службы поддержки банка по телефону или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕДОСТУПНОСТИ СЧЕТА



- в отделении банка
- в личном кабинете клиента
- на сайте в личном кабинете

3 СРАЗУ ЖЕ ПОДНЯТЬ ВОПРОСЫ



- на сайте банка
- по телефону
- на официальном сайте банка
- в личном кабинете

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ

- свои данные карты и личный код
- не делайте скриншоты паролей
- не сообщайте никому код подтверждения
- не сообщайте данные от имени банка

НЕ ПУБЛИКУЙТЕ

фото или видео документов в интернете для фото

УСТАНОВИТЕ

защитные приложения

КОДОВОЕ СЛОВО

не сообщайте никому и никому не сообщайте свои данные, связанные со счетом



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, киберпреступники могут похитить. Все данные с ваших счетов.



КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАИЖЕНО?

- Появились уведомления о подозрительных действиях
- Сильно замедлился процесс работы приложения
- Появились уведомления о краже
- Телефон часто перегревается

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- Позвоните в Банк и сообщите о подозрительных действиях в личном и мобильном Банке и все карты, которые использовались на устройстве
- Обратитесь в сервисный центр, чтобы выслать телефон
- Переинсталируйте карты, особенно карты в Банке, из мобильного Банка и удалите приложения банковских переводов

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- Обновляйте операционную систему и приложения на устройствах
- Не устанавливайте на устройства из неизвестных, не установленных программ на их сайты и не используйте чужие файлы
- Скрывайте персональные данные на приватных устройствах
- Обновляйте идентификацию на своем устройстве
- Не используйте приложения от P-услуг