
КАК ЗАЩИТИТЬ
СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ
ВИРУСЫ:
• открывают удаленный доступ к вашему устройству
• крадут логины и пароли от онлайн- и мобильного банка
• перехватывают 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
Показывает всплывающие окна
Тормозит объем памяти
ЧТО ДЕЛАТЬ,
ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?
Позвоните в банк и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
Обратитесь в сервисный центр, чтобы вылечить гаджет
Перевыпустите карты, смените логин и пароль от онлайн-банка и заново установите банковское приложение
КАК ЗАЩИТИТЬ
УСТРОЙСТВО ОТ ВИРУСОВ?
Используйте антивирус и регулярно его обновляйте
Не переходите по ссылкам от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
Скачивайте приложения только из проверенных источников
Обновляйте операционную систему устройства
Избегайте общедоступных Wi-Fi сетей


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 ОПЕРАЦИЕЙ
Заявление должно быть написано:
• в течение суток после сообщения о списании денег
• на месте в отделении банка
3 ОБРАТИТЬСЯ
В ПОЛИЦИЮ
Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают
КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?
НИКОМУ НЕ СООБЩАЙТЕ:
• срок действия карты и трехзначный код на ее обратной стороне (CVV/CVC)
• пароли и коды из уведомлений
• логин и пароль от онлайн-банка
КОДОВОЕ СЛОВО
называйте только сотруднику банка, когда сами звоните на горячую линию
НЕ ПУБЛИКУЙТЕ
персональные данные и открытый доступ
УСТАНОВИТЕ
антивирусы на все устройства
Банк не компенсирует потери, если вы нарушили правила безопасного использования карты


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 ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, 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
Дизайн скопирован некачественно, 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

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

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