

Банк России

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 использование оооо
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- **Позвоните в банк** и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовались на устройстве
- **Обратитесь в сервисный центр**, чтобы выключить гаджет
- **Перезагрузите карты, смените логины 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 файлы
- Скачивайте приложения только на **проверенных источниках**
- **Обновляйте** операционную систему устройства
- **Используйте** общедоступных Wi-Fi сетей

 Подробнее о защите гаджетов читайте на vcbr.ru

 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 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 подаст заявление, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и предельный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из SMS-сообщений
- логины и пароли от онлайн-банка

НЕ ПУБЛИКУЙТЕ персональные данные в открытом доступе

УСТАНОВИТЕ антивирусы на все устройства

КОДОВОЕ СЛОВО называйте только сотруднику банка, когда сами увидите на горючую линию

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

 Подробнее о правилах безопасности читайте на vcbr.ru

 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 два капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, SMS, сообщений в соцсетях или мессенджерах, рекламе, объявлениях 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
- Данные сотрудников неизвестны, 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 точную сумму прямо перед оплатой

 Подробнее о правилах кибербезопасности читайте на vcbr.ru

 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
Ссылаясь на многократно опубликованные материалы о деятельности международных корпораций, Трестов Высшего Общества – «Глобал-Обанк», заманивают на распродажи.

ОТКАЗЫВАЮТСЯ ОТ СВОИХ ДОЛГОВ
Ссылаясь на якобы наличие долгов и обязательств перед банком, предлагают услуги.

СПЕКУЛИРУЮТ НА ГРОМКИХ СОВЕТАХ
Внезапно объявляют об открытии нового банка, предлагают услуги, предлагают услуги, предлагают услуги.

МАСКИРУЮТСЯ
Предлагают услуги, предлагают услуги, предлагают услуги.

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его.
2. Закажите оригинальную банковскую карту для оплаты в интернете и используйте ее только для оплаты.
3. Всегда проверяйте адрес электронной почты и сайта – не переходите по ссылкам от неизвестных людей.
4. Не переходите по ссылкам от неизвестных людей.
5. Никогда не сообщайте свои персональные данные.

 Подробнее о правилах безопасности читайте на banki.ru/ru/infocenter

 Финансовая культура

 МВД РОССИИ ПРЕДУПРЕЖДАЕТ

НЕ ОТКРЫВАЙТЕ ДВЕРЬ НЕЗНАКОМЫМ
людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиник, ЖКХ и т.д. Позвоните и уточните, направляли ли к Вам этого специалиста!



НЕ ДОВЕРЯЙТЕ,
если Вам звонят и сообщают, что Ваш родственник или знакомый попал в аварию, за решетку, в больницу или совершил ДТП, и теперь за него нужно внести залог, штраф, возмездие, купить дорогие лекарства – в общем испугаться. **ЭТО ОБМАН!**



**БУДЬТЕ
БДИТЕЛЬНЫ!**

**Звоните в полицию
02/102**

Бесплатная
"горячая линия МВД России"
8-800-222-74-47

Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам?
НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!

 Банк России

 Министерство внутренних дел Российской Федерации

 Федеральная служба безопасности Российской Федерации

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1. **НА ВАС ВЫХОДЯТ САМИ**
Аферисты могут представляться службой безопасности банка, налоговой, прокуратурой.
2. **РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ Пугают**
Сильные эмоции притупляют бдительность.
3. **ЗВОНЯТ**
Из банка, налоговой, прокуратуры.
4. **УБЕДИТЕСЬ, что это не мошенники!**
5. **НА ВАС ДАВЯТ**
Аферисты всегда притупляют у вас не было времени все обдумать.
6. **ГОВОРЯТ О ДЕНЕГАХ**
Предлагают деньги, обещают получить компенсацию или участие в инвестиционном проекте.
7. **ПРОСЯТ СООБЩИТЬ ДАННЫЕ**
Злоумышленники пытаются получить 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 сообщить 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
- данные о карте
- персональные данные

 Как защитить свои финансы, читайте на banki.ru/ru/infocenter

 Финансовая культура