Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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

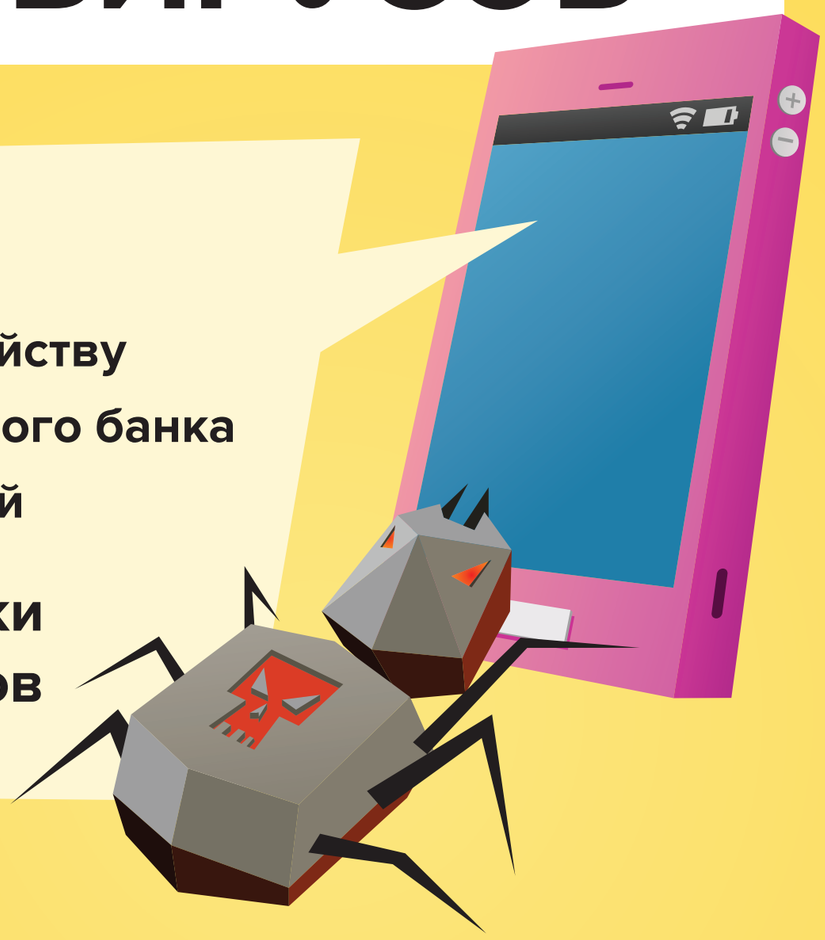
Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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
- 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 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

Подробнее о защите гаджетов читайте на fincult.info

Финансовая культура

ЧИТАЙТЕ ТАКЖЕ НА САЙТЕ FINCULT.INFO

Личные финансы:
С чего начать путь инвестора?
Как распознать финансовую пирамиду?
Для чего вести учет доходов и расходов?

Малый бизнес:
Как получить кредит на бизнес?
Как начать свое дело и преуспеть?
Как открыть ИП и не запутаться в документах?

Понятная экономика:
Почему растут цены?
Кто решает, сколько стоит валюта?
Почему нельзя напечатать денег, чтобы всем хватило?

Банк России

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

ЗАЩИТИТЕ СЕБЯ И СВОЮ СЕМЬЮ

Кто охотится за вашими деньгами?
Как распознать мошенников?
Что делать, если вас все-таки обманули?

Контактный центр Банка России

8 800 250-40-72

(для бесплатных звонков из регионов России)

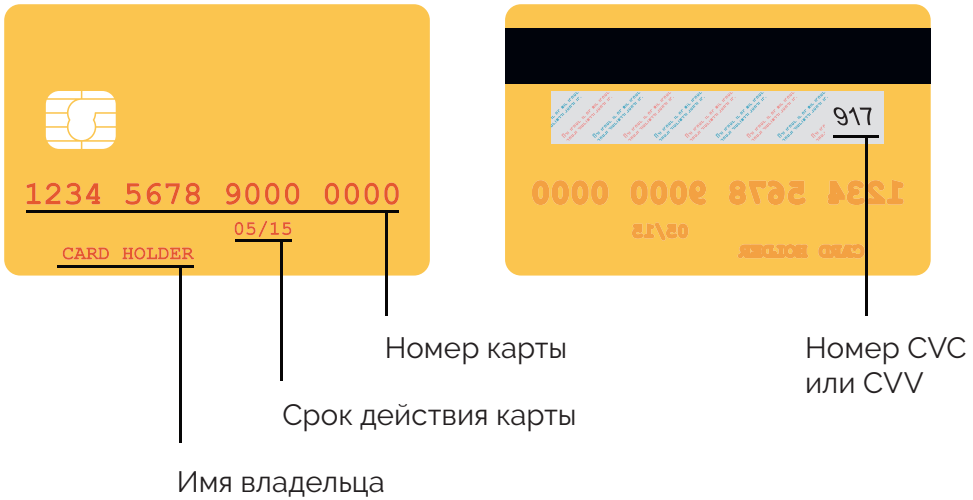
Интернет-приемная Банка России
cbr.ru/reception

fincult.info — сайт для тех, кто думает о будущем

Мошенники умеют выманивать деньги по телефону, в социальных сетях и офисах. Как они это делают?

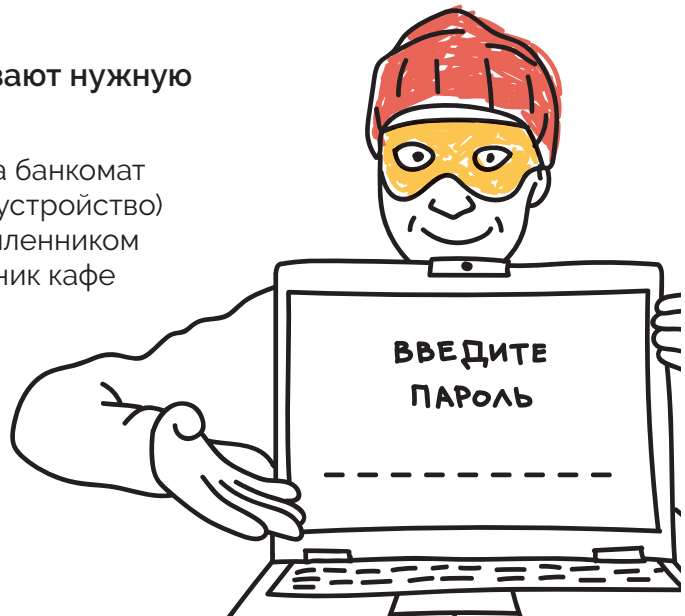
МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам нужны ваши данные:



Как мошенники добывают нужную информацию?

Они могут установить на банкомат скиммер (считывающее устройство) и видеокамеру. Злоумышленником может оказаться сотрудник кафе или магазина, который получит доступ к вашей карте хоть на пять секунд.



БИНАРНЫЕ ОПЦИОНЫ

Не связывайтесь с бинарными опционами. Кажется, все просто: нужно открыть счет и делать ставки на рост или падение стоимости валют. Если угадали, вы зарабатываете, если нет — теряете деньги.

Но сегодня в интернете нет площадок, на которых могут проводиться эти сделки, поэтому все обещания о легком заработке на бинарных опционах — мошенничество.

Вы просто потеряете деньги.

Если вы все же решили выйти на рынок Форекс, внимательно изучите закон и «Базовый стандарт совершения операций на финансовом рынке при осуществлении деятельности форекс-дилера».

У форекс-дилера обязательно должна быть лицензия. Уточнить, есть ли она, можно на сайте Банка России.

Компания должна быть зарегистрирована в России, а не в офшорных зонах.

Предупредите пожилых родственников, что агрессивная реклама быстрого заработка в интернете — мошенничество.

А еще лучше — не рискуйте, попробуйте начать путь инвестора на бирже.

Если вы стали жертвой мошенничества на финансовых рынках

Соберите все документы (договоры, заключенные с посредником, чеки на перевод денег), сделайте скриншоты с сайта — и обратитесь в полицию.

Сообщите в Банк России.

КАК УБЕРЕЧЬСЯ ОТ ОБМАНА

Финансовая организация должна иметь лицензию Банка России. Сверьтесь со Справочником участников финансового рынка на сайте cbr.ru.

Проверьте компанию в Едином государственном реестре юридических лиц ФНС России.

Запросите образцы договоров, копии документов. Проконсультируйтесь с юристом.

Я ВЛОЖИЛСЯ И ПРОГОРЕЛ. ЧТО ДЕЛАТЬ?

Составьте претензию и направьте ее в адрес компании.

Если компания отказывается вернуть деньги, соберите все документы и обратитесь в полицию.

Свяжитесь с юристом и попробуйте найти других жертв мошенничества.

МОШЕННИКИ НА РЫНКЕ ФОРЕКС

Торговля на рынке Форекс — риск, гарантий нет, больше шансов потерять все, чем сорвать куш. Но опасность кроется и в посредниках. Чтобы обычному человеку выйти на рынок Форекс, нужно заключить договор с посредником, форекс-дилером, и торговать через него. Можно нарваться на мошенников, которые возьмут у вас деньги и не вернут их.

КАК НЕ ПОПАСТЬСЯ

Осмотрите банкомат. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.

Набирая ПИН-код, прикрывайте клавиатуру рукой.

Подключите мобильный банк и СМС-уведомления.

Если совершаете покупки через интернет, никому не сообщайте секретный код из СМС.

Никогда не теряйте из виду вашу карту.

МЕНЯ ОБОКРАЛИ. ЧТО ДЕЛАТЬ?

Позвоните в банк (номер есть на обороте карты или на главной странице сайта банка) и заблокируйте карту.

Запросите выписку по счету и напишите заявление о несогласии с операцией.

Обратитесь с заявлением в полицию.

КИБЕРМОШЕННИЧЕСТВО

Вам приходит СМС или письмо «от банка» со ссылкой, просьбой перезвонить или уведомлением о крупном выигрыше. Или звонят «из банка» и просят сообщить личные данные. Или пишут в социальных сетях от имени родственников или друзей, которые попали в беду, и просят перевести деньги на неизвестный счет. Скорее всего, вы имеете дело с мошенниками.

КАК НЕ ПОПАСТЬСЯ

Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам.

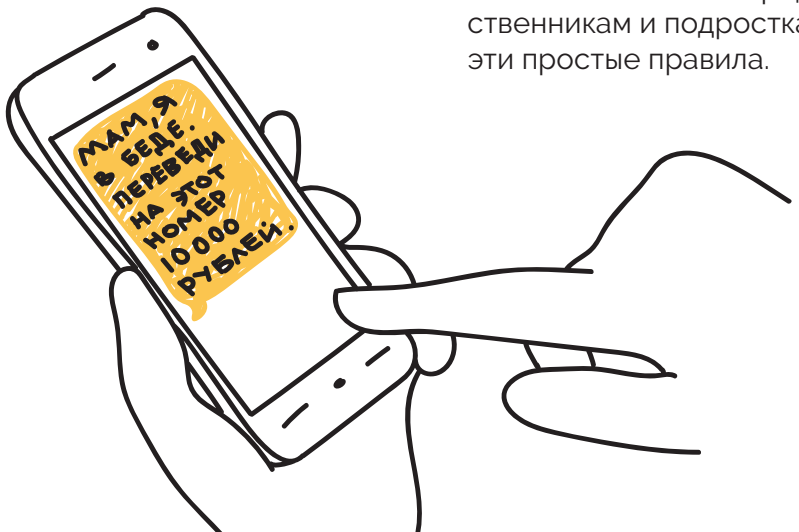
Никому не сообщайте персональные данные, тем более пароли и коды.

Не храните данные карт на компьютере или в смартфоне.

Проверяйте информацию. Если вам звонят и сообщают что-то о вашем счете (по ошибке списали или зачислили деньги), не следуйте никаким инструкциям, срочно звоните в банк.

Установите антивирус на компьютер себе и родственникам.

Объясните пожилым родственникам и подросткам эти простые правила.



С МОЕЙ КАРТЫ ОБМАНОМ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

Позвоните в банк и заблокируйте карту.

Обратитесь с заявлением в полицию.

ФИНАНСОВЫЕ ПИРАМИДЫ

Они маскируются под микрофинансовые организации, инвестиционные и управляющие предприятия, онлайн-казино. Заявляют о высоких процентах по вкладам и отсутствии рисков, гарантируют доход (что запрещено на рынке ценных бумаг), обещают помощь людям с плохой кредитной историей.

Заработать на пирамидах нельзя. Если вы вложите деньги, вы их потеряете.

Прокуратура Хилокского района разъясняет

Основные причины роста **IT-преступлений:** доверчивость, юридическая и информационная неграмотность граждан, желание приумножить имеющиеся денежные средства, получить различного рода компенсации или иной дополнительный доход.

Основные способы обмана:

Звонки о необходимости перевода Ваших денежных средств на «сохранные» счета банков, во избежание их хищения либо неправомерного оформления кредитов третьими лицами.

Предложения о получении различных выплат и компенсаций из учреждений банковского сектора, в том числе по снижению процентной ставки по кредитам, а также получения кредита без справок и поручителей.

Звонки от сотрудников правоохранительных органов, Федеральной службы безопасности, прокуратуры, иных государственных органов с требованиями, рекомендациями, советами о переводе денег на иные счета, сообщения персональных данных.

Сообщения, телефонные звонки о том, что родственник попал в беду, с просьбой выдачи или перевода денежных средств на лечение или избежания негативных последствий в виде задержания, привлечения к ответственности и т.п.

Предложения о получении дополнительного дохода от инвестирования денежных средств на ложных биржевых площадках, находящихся в сети Интернет.

Установка приложений удаленной (дистанционной) работы или переход по ссылке, влекущей доступ злоумышленников ко всем данным, хранящимся в телефоне и компьютере.

Объявления о купле, продажи товаров посредством сайтов объявлений.

Сообщение от знакомых, родственников в мессенджерах Viber, WhatsApp, Telegram с просьбой срочно занять денежные средства.

Помните! Мошенники обладают навыками убеждения!

Незамедлительно прервите разговор или переписку, при наличии сомнений обратитесь в банковские организации за уточнением сведений о движении Ваших денежных средств, свяжитесь с родственниками или знакомыми, о которых идет речь, а при наличии угроз, конкретных требований о выдаче денег или переводе на иные счета, установке каких-либо программ на телефон или компьютер – сообщайте в органы полиции.

Мошенничества такого рода предотвратить не сложно, если быть внимательными, бдительными и информированными!