



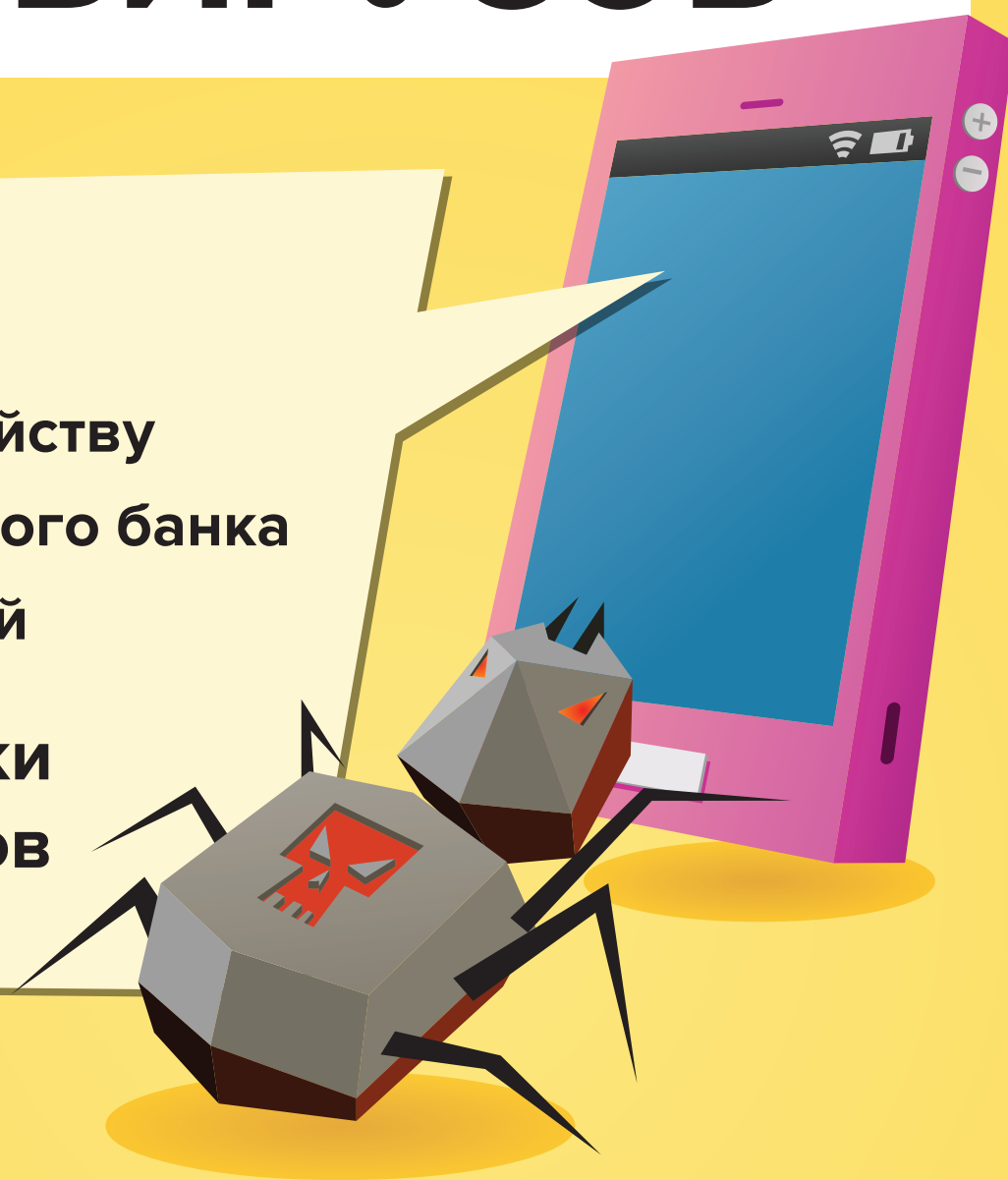
Банк России

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 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





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?

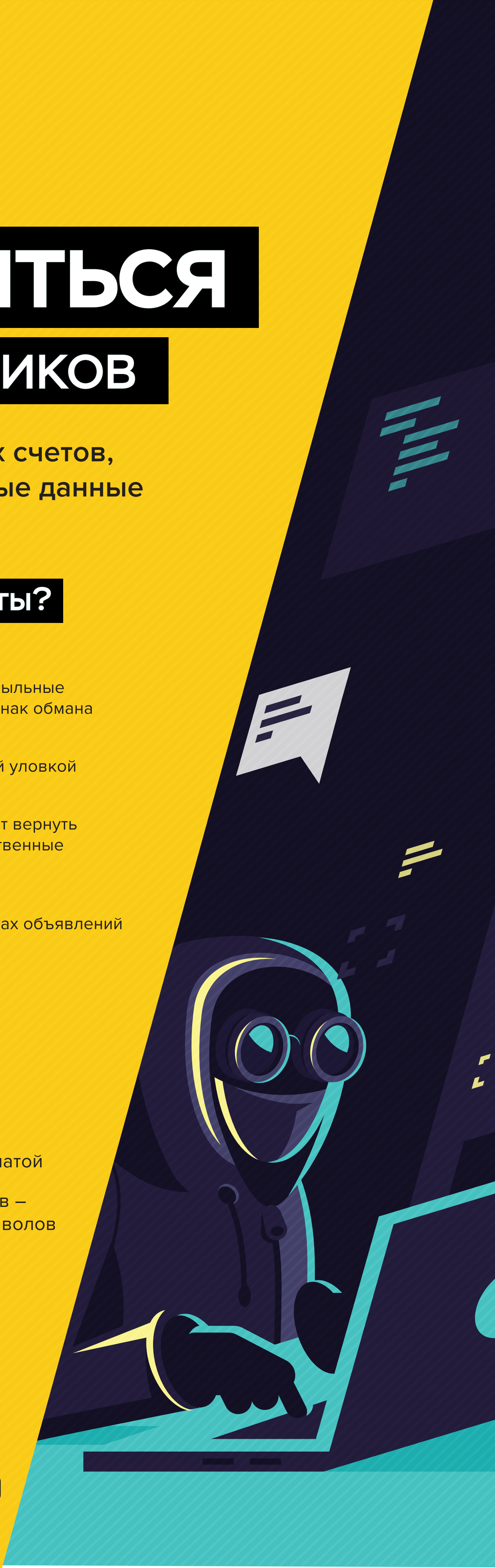
- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам 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

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 поймут

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию



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



Подробнее о правилах безопасности
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





СМС, МЕССЕНДЖЕРЫ, СОЦСЕТИ



Вам пришло СМС от банка с информацией:

- о заблокированном платеже или карте;
- о выигрыше;
- об ошибочном переводе на ваш банковский счет или мобильный телефон с просьбой вернуть деньги.

— *Что делать?*



**НЕ ПЕРЕХОДИТЕ
ПО ССЫЛКЕ И
НЕ ПЕРЕЗВАНИВАЙТЕ!**

Проверьте информацию, позвонив в банк по номеру, который указан на вашей банковской карте.



Знакомый в соцсетях просит дать в долг или перевести деньги на лечение.

— *Что делать?*



**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ СРАЗУ!**

Пerezвоните своему знакомому, чтобы выяснить ситуацию, — возможно, его страницу взломали.



Контактный центр Банка России

8 800 300-30-00
(бесплатно для звонков
из регионов России)

+7 499 300-30-00
(в соответствии с тарифами
вашего оператора)

300
(бесплатно для звонков
с мобильных телефонов)

Все представленные номера
доступны для звонков
круглосуточно

**Банк России
не совершает исходящих
звонков
с указанных номеров**



fincult.info

ПОРА УЗНАТЬ ПРО ДЕНЬГИ ВСЕ



Банк России



**ОСТОРОЖНО:
МОШЕННИКИ!**

**НИКОГДА
НЕ СООБЩАЙТЕ
НЕЗНАКОМЫМ ЛЮДЯМ
ТРЕХЗНАЧНЫЙ КОД
НА ОБОРОТЕ КАРТЫ, PIN-КОД
И ПАРОЛИ ИЗ СМС**



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО



Звонят из банка. Говорят об угрозе вашим деньгам на счете и просят перевести деньги на другой счет. Спрашивают данные карты.

— *Что делать?*



СРАЗУ ПОЛОЖИТЕ ТРУБКУ — ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.



Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

— *Что делать?*



НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

Если во время разговора вас просят совершить платеж — это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.



Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

— *Что делать?*



ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите имя, фамилию звонящего и название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.



ИНТЕРНЕТ



Предлагают вложить деньги на очень выгодных условиях.

— *Что делать?*



**ОТКРОЙТЕ САЙТ
WWW.CBR.RU/FINORG**

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.



На сайтах с объявлениями («Авито», «Юла» и т.п.) предлагают товары и услуги по заниженным ценам.

— *Что делать?*



НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлениями.



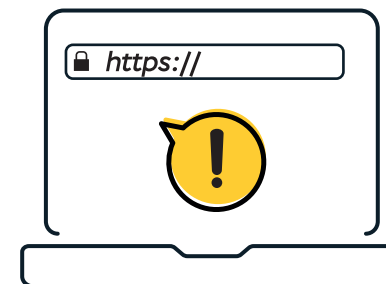
Нужно перевести деньги или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

— *Что делать?*



ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надпись **https://** и «**замочек**» в адресной строке браузера.



Как взять кредит и не увязнуть в долгах



Кредит — удобный финансовый инструмент, если знать, как им правильно пользоваться. Однако заемные деньги требуют ответственности и дисциплины. Чтобы не оказаться в долговой яме, следуйте шести главным правилам:



Трезво оценивайте свои финансовые возможности

Сделайте паузу и подумайте, насколько вам нужны заемные деньги, можно ли обойтись без них и как вы будете возвращать полученную сумму.



Не берите кредит в первом же банке

Сравните условия в нескольких банках, чтобы подобрать максимально подходящий кредит. Если вы студент или пенсионер, сообщите об этом сотруднику банка: возможно, для вас действуют особые предложения.



Помните о своих правах

Берите кредит или заем только в организациях, у которых есть лицензия Банка России. В этом случае ваши права будут защищены. Не связывайтесь с черными кредиторами: они выбивают долги в прямом смысле слова.



Подписывайте договор, только если все условия понятны

Обращайте внимание на комиссии, штрафы за просрочку платежей, дополнительные условия, например страхование. От навязанного полиса вы можете отказаться в период охлаждения, который действует в течение 14 календарных дней с момента покупки. Но учтите, что после отмены страховки ставка по кредиту может вырасти.



Не тяните с погашением долга

Соблюдайте график выплат и не откладывайте платеж на последний момент. Имеет смысл вносить деньги за 5–7 рабочих дней до даты погашения, чтобы они точно успели поступить на кредитный счет.



Убедитесь, что кредит закрыт

После последнего взноса получите справку в банке о том, что вы больше ничего не должны.



Банк России



Финансовая культура

Узнай больше на fincult.info



Личный финансовый план



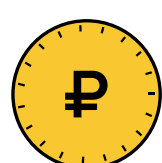
Финансовый план нужен не для бесконечной экономии, а чтобы получать больше за те же деньги. Он помогает быстрее достигать цели: купить машину, отправиться в отпуск или сделать ремонт.

Как составить толковый план?

- 1 Сформулируйте цели**
Сделайте это честно и четко, укажите реальные суммы и сроки, в которые хотите достигнуть желаемого.
- 2 Расставьте приоритеты**
Возможно, покупка автомобиля подождет. Зато починить систему отопления дома нужно успеть до наступления холодов.
- 3 Оцените бюджет**
Подсчитайте свои доходы и расходы и поймете, сколько вы сможете откладывать на свою цель каждый месяц без ущерба для себя.
- 4 Рассмотрите все варианты финансирования**
В каких-то случаях поможет сверхурочная работа и оптимизация расходов. В крайнем случае возьмите кредит или заем, но реально оцените свои силы. В идеале на погашение долгов должно уходить не более 30% вашего ежемесячного дохода.
- 5 Попробуйте инвестировать**
Это может принести вам дополнительные деньги, но помните о рисках: чем выше потенциальная прибыль, тем больше шансов все потерять. Неопытным инвесторам лучше выбирать надежные инструменты, например облигации федерального займа. Но важно помнить, что инвестиции, в отличие от банковских вкладов, не застрахованы государством.



Банк России



Финансовая
культура

Узнай больше на fincult.info



Как не попасться на уловки мошенников



Чтобы обезопасить свои деньги от злоумышленников, придерживайтесь главных принципов кибербезопасности:

1

Держите в секрете конфиденциальные данные

Никому не сообщайте полные реквизиты карты, включая срок ее действия и три цифры с оборота, а также пароли и коды из банковских уведомлений. Ими интересуются только мошенники.

2

Не спешите выполнять инструкции незнакомцев

Не переходите по ссылкам неизвестных отправителей, не переводите деньги по первому требованию (даже если вас об этом просит друг или родственник – возможно, это мошенники, взломавшие их аккаунты). Не перезванивайте на неизвестные номера и не вводите данные карты на подозрительных сайтах.

3

Перепроверяйте информацию

Получили внезапный тревожный звонок «из банка»? Не верьте собеседнику на слово. Чтобы прояснить ситуацию, положите трубку и вручную наберите номер банка, указанный на вашей карте или на его официальном сайте.

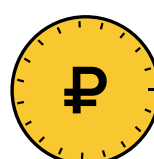
4

Защищайте данные на своих устройствах

Установите антивирус на все гаджеты, которыми пользуетесь, и не забывайте его обновлять. Ставьте надежные пароли на вход в аккаунты, к которым привязана ваша банковская карта. Используйте биометрическую разблокировку для телефона – мошенники не смогут ее подделать, если вы потеряете устройство.



Банк России



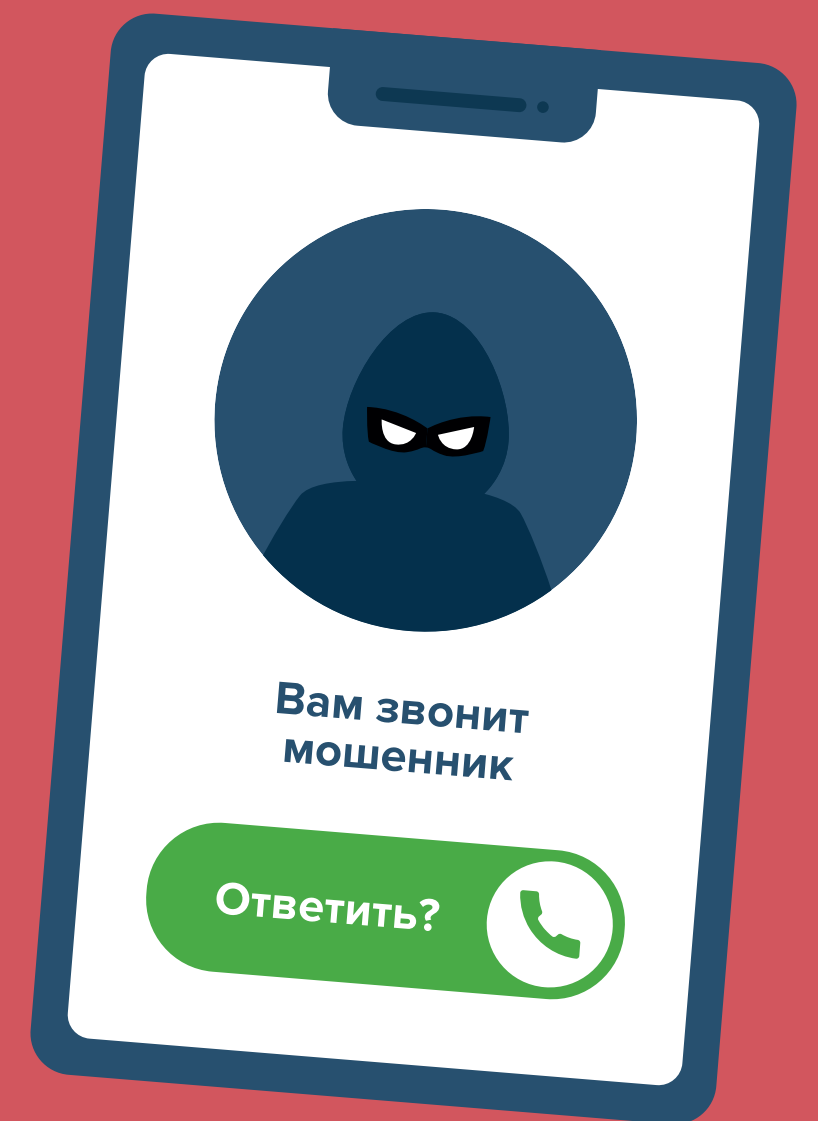
Финансовая
культура

Узнай больше на fincult.info



Осторожно: телефонное мошенничество

Звонят из банка, полиции или другой организации? Просят перевести деньги на безопасный счет или назвать данные карты, пароли из банковских уведомлений, персональные данные? Это мошенники.



Как обезопасить свои деньги?

Положите трубку и перепроверьте информацию. По любым операциям с картами и банковским счетом звоните в свой банк сами. Вручную наберите номер банка, указанный на обороте карты или на его официальном сайте. Только там вам прояснят ситуацию.

Обратите внимание на признаки, которые помогут быстро распознать мошенников:

На вас выходят сами.

Аферисты могут представиться кем угодно: службой безопасности банка, налоговой, прокуратурой. Но они всегда иницируют общение сами. Если вы получили подозрительный звонок, СМС или письмо – насторожитесь.

С вами говорят о деньгах.

Схемы обмана почти всегда связаны с финансами: вам обещают золотые горы, предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно вложиться» (на самом деле — в финансовую пирамиду).

Просят сообщить данные.

Мошенники любыми способами пытаются выманить секретные данные карты, включая срок действия и три цифры с оборота, а также пароли и коды из банковских уведомлений. Настоящий сотрудник банка никогда ими не интересуется.

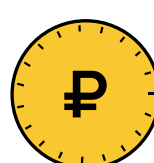
На вас давят.

Аферисты всегда торопят, чтобы у вас не было времени обдумать ситуацию. Провоцируют сильные эмоции, стараясь сбить с толку. Например, сообщают: «Ваш онлайн-банк взломали!», чтобы вы от растерянности и волнения безоговорочно следовали их инструкциям, лишь бы спасти свои деньги.

Не всегда при общении с аферистом вы заметите все пять признаков мошенничества. Но в любой ситуации стоит проявить бдительность.



Банк России



Финансовая
культура

Узнай больше на fincult.info





Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



НЕ ОТДАВАЙТЕ КАРТУ В ПЛОХИЕ РУКИ!

КТО ТАКИЕ ДРОППЕРЫ

Это сообщники злоумышленников, которые выводят и обналичивают похищенные у граждан деньги.



ЧЕМ ЗАНИМАЮТСЯ ДРОППЕРЫ

- Получают на свои карты деньги от незнакомцев и передают их другим лицам – наличными или переводом
- Предоставляют злоумышленникам банковские карты или доступ к онлайн-банку
- Принимают наличные деньги от неизвестных людей, вносят их на свои счета для последующего перевода

ГДЕ И КАК ИЩУТ ДРОППЕРОВ

Основной канал – интернет (социальные сети, мессенджеры, электронная почта).

Злоумышленники обещают гарантированный доход без официального трудоустройства и удаленный режим работы. Опыт работы и специальные навыки их не интересуют.

Единственное требование к дропперу – наличие банковских карт.

ЧТО ГРОЗИТ ДРОППЕРАМ

- ! Дропперы попадают в базу данных Банка России
- ! Банки ограничивают им доступ к онлайн-банку и картам
- ! Для многих граждан такая «работа» заканчивается уголовным наказанием