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 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

**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 поймают

# 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

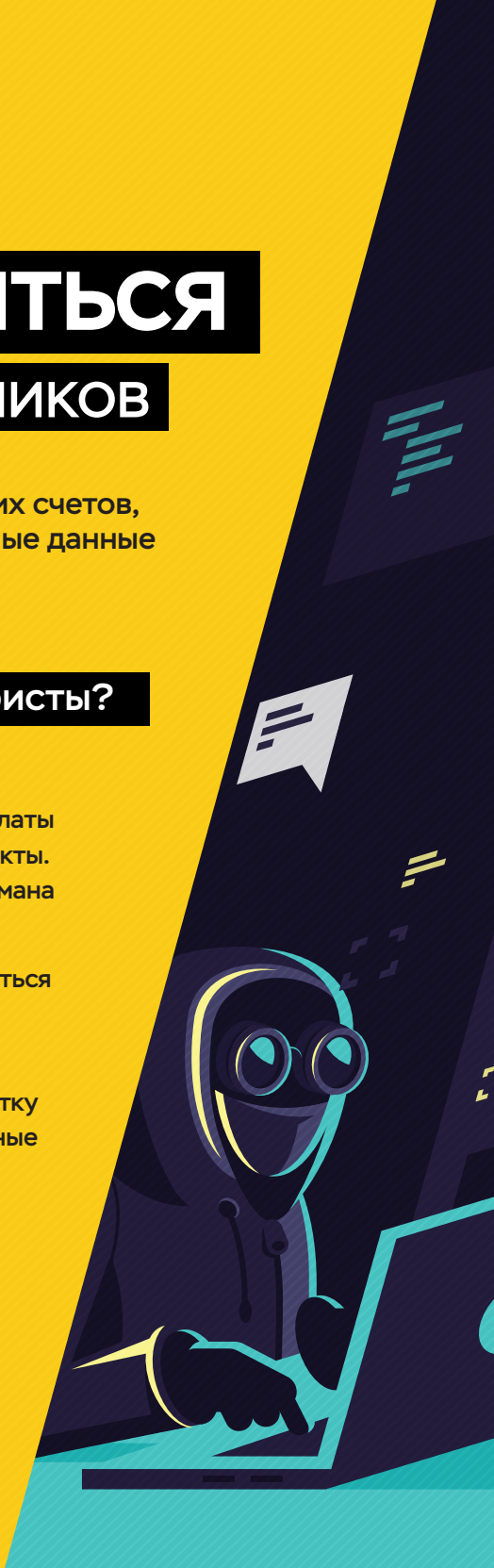
Финансовая культура

Банк России

# 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

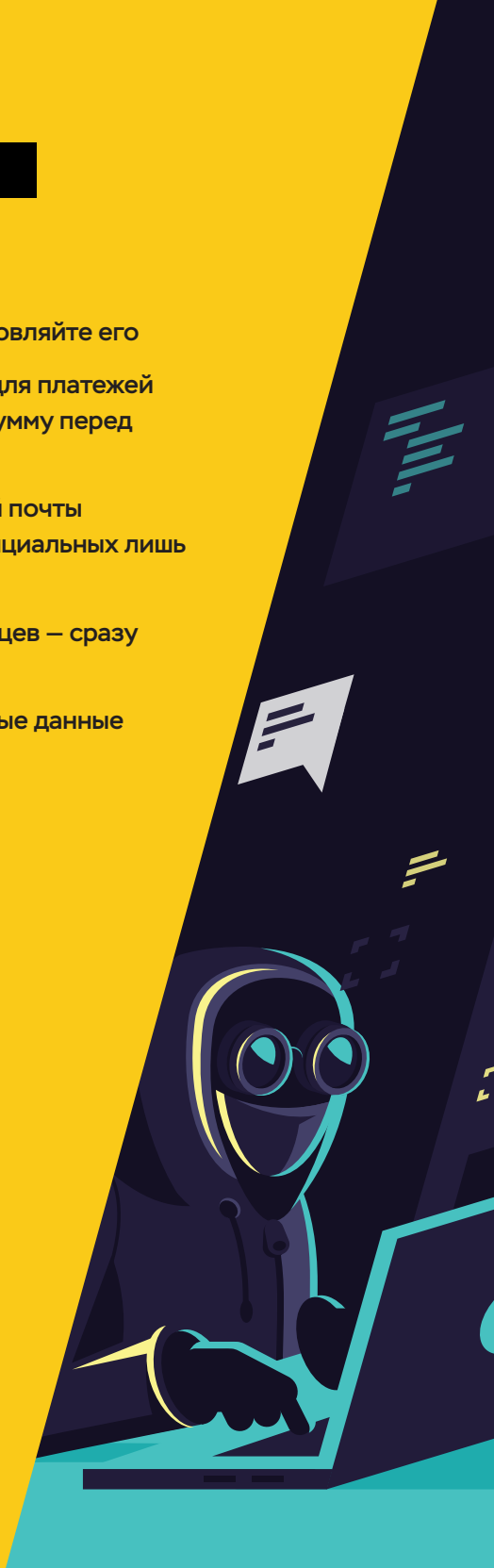
**ЗАМАНИВАЮТ НА РАСПРОДАЖИ**
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

**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**

# ФИНАНСОВОЕ МОШЕННИЧЕСТВО

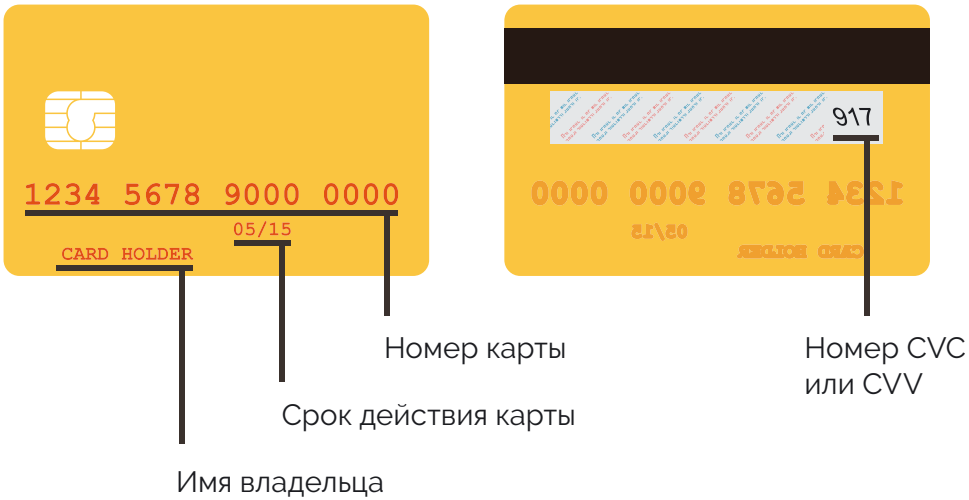
## ЗАЩИТИТЕ СЕБЯ И СВОЮ СЕМЬЮ

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

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

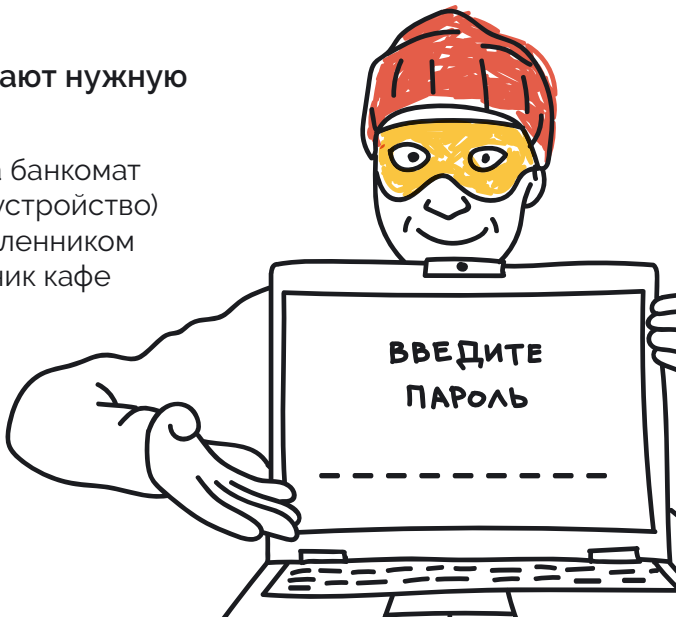
# МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

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.



# 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

**Главное правило — не торопитесь и всегда проверяйте информацию.**

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

Никому не сообщайте личные данные (из паспорта и других документов) и полные данные карты, включая три цифры с оборота и срок действия.

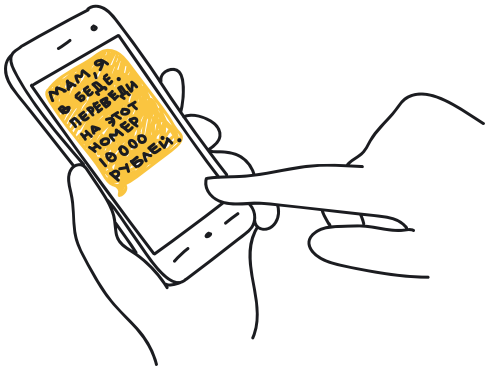
Не храните реквизиты карт и личные данные на компьютере или в смартфоне и не вводите их на подозрительных сайтах.

Скачивайте приложения только в официальных онлайн-магазинах.

Установите и регулярно обновляйте антивирусы на всех устройствах.

Не пользуйтесь непроверенными сетями Wi-Fi.

Расскажите про эти простые правила своим родственникам и знакомым.



# С МОЕЙ КАРТЫ ОБМАНОМ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

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

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

**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.**

## 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.

# 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 и на деле обернется потерей денег.

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.

# 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

Контактный центр Банка России

**8 800 300-30-00**

(для бесплатных звонков
из регионов России)

Интернет-приемная
Банка России
**cbr.ru/reception**

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

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**

# ОСТОРОЖНО:

## телефонные мошенники!
## 5 признаков обмана

Финансовая культура

# 1 На вас выходят сами

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой или Центробанком.

Любой подобный звонок, СМС или письмо – повод насторожиться.

# 2 Радуют внезапной выгодой или пугают

Сильные эмоции притупляют бдительность.

# 3 На вас давят

Мошенники всегда торопят, чтобы у вас не было времени все обдумать.

# 4 Говорят о деньгах

Предлагают спасти сбережения, перевести деньги на специальный счет в Центробанке, получить компенсацию или вложиться в инвестиционный проект.

# 5 Просят сообщить данные

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений.

# Сотрудники банков и полиции никогда не спрашивают:

- реквизиты карты
- пароли из СМС
- персональные данные

**И никогда не просят переводить деньги с вашей карты!**

# Никогда никому не сообщайте:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV\CVC)
- пароли/логины к приложению или онлайн-банку
- ПИН-код
- кодовое слово
- персональные данные

# 5 примет, по которым можно вычислить мошенников

Финансовая культура

# 1 Незнакомец неожиданно связывается с вами сам

Например, от имени банка, полиции, магазина. Способы могут быть разные — звонок, СМС или ссылка в мессенджере.

Общее у них одно — кто-то сам вышел на связь с вами. Значит, ему что-то от вас нужно.

# 2 С вами говорят о деньгах

Основная задача мошенников — получить доступ к чужим деньгам.

Вам могут предложить:

- перевести все деньги на «безопасный счет»
- оплатить «страховку для получения кредита»
- «очень выгодно» инвестировать свои сбережения.

И многое другое. Главное:

**речь всегда будет идти о деньгах.**

# 3 Вас просят сообщить данные

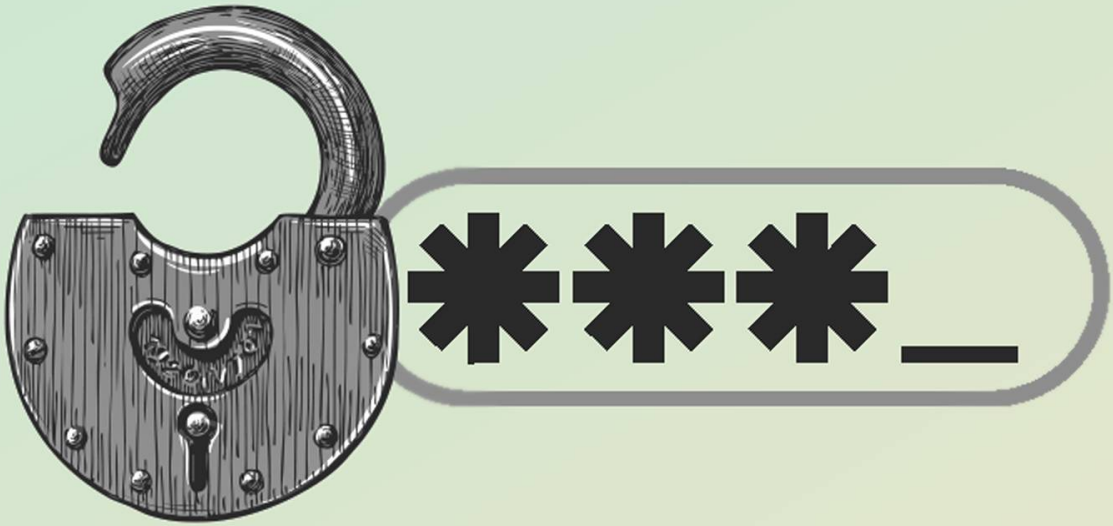
Обычным ворам нужен ключ от квартиры, мошенникам — «ключ» от вашего счета:

срок действия карты и cvc-код

логины и пароли к приложению банка или личному кабинету на сайте

коды из банковских уведомлений.

Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли.




Если о них спрашивают — будьте уверены, звонят не из банка и вас точно пытаются обмануть.

# 4 Вас выводят из равновесия

Мошенники стремятся
вызвать у вас сильные
эмоции — напугать или обрадовать.
Например, сообщают:


чтобы вы растерялись
и выдали любую информацию,
лишь бы спасти деньги.

Еще вас могут обрадовать внезапным «выигрышем в лотерею». Взамен нужно лишь оплатить комиссию на сайте.

С которого, конечно, мошенники уведут данные вашей карты.

Не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.

## 5 На вас давят:

 торопят

 принуждают к чему-то

 ставят условия:
«сейчас или будет поздно».

Такие ситуации подозрительны.
Поэтому общение лучше
прекратить сразу.

Никогда не принимайте поспешных решений, особенно если они касаются ваших денег.

Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить реальное положение дел.

Финансовая культура

# Будьте бдительны, не поддавайтесь на уловки мошенников!