



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ

# 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](http://fincult.info)



Финансовая  
культура



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](http://fincult.info)



Финансовая  
культура



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ

# 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 ОКАЗТЬСЯ 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](http://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 обратной 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](http://fincult.info)



Финансовая  
культура



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ

# 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](http://fincult.info)



Финансовая  
культура

УМВД России по Омской области предупреждает  
Осторожно – мошенники!!!

Вам позвонили из Банка с номеров телефонов начинающихся со следующих цифр и представились сотрудниками службы безопасности банка:

**+7-495-XXX-XX-XX    +7-499-XXX-XX-XX    +7-800-XXX-XX-XX    +7-900-XXX-XX-XX**

или с ДРУГИХ неизвестных номеров и уверенным голосом, профессиональным «языком» сообщили о том, что со СЧЁТА банковской карты:

- была попытка перевода денег;
- совершаются мошеннические действия;
- кто-то пытается похитить деньги;
- была попытка несанкционированного списания денег;
- осуществляется подозрительная транзакция, либо какая-то активность;
- осуществляется попытка входа в личный кабинет;
- осуществлена покупка в Интернет-магазине;
- пришла заявка на перечисление на имя неизвестного лица;
- необходимо провести проверку банковских карт с целью защиты их от мошенников;
- осуществляется перевод в другой город;
- произошел взлом доступа к счёту.

Мошенники не редко называют потерпевших по имени, отчеству и в целях защиты денежных средств просят назвать, в некоторых случаях «роботу», НОМЕР банковской карты, срок действия, CVC, CVV пароли, которые представляют с собой три цифры, указанные с обратной стороны банковской карты, а затем просят СООБЩИТЬ ПАРОЛИ, которые поступают в смс-сообщения от Банка на номер мобильного телефона потерпевшего.

**НЕ ВЕРЬТЕ, ЭТО ОБМАН!!!**

- Не сообщайте свои персональные данные, реквизиты банковской карты, коды и другие пароли, дающие доступ к Вашей карте;
- Даже если номер, с которого звонит «сотрудник банка» совпадает с официальным номером Банка, не верьте этому, злоумышленники могут использовать технологию подмены номеров.
- Завершите вызов и наберите номер банка, указанный на Вашей банковской карте.

Если Вы стали жертвой мошенников, либо подозреваете, что можете ею стать, незамедлительно обратитесь в полицию. Звоните «02», с мобильного «102», или «112».

## **Как сохранить сбережения на банковском счете и не стать жертвой мошенников?**

**Вам звонят и представляются сотрудником банка  
и уверенным голосом говорит:**

- Произошла попытка перевода денежных средств с вашей банковской карты;
- Просят установить на мобильный телефон какие-либо приложения;
- Предлагают сообщить персональные данные, номер карты и три цифры CVV кода расположенного с обратной стороны банковской карты;
- Просят проследовать в ближайший банкомат для перевода денежных средств на резервный счет.

### **ПОМНИТЕ ЭТО ОБМАН !!!**

- Сотрудники банка ни когда не присылают писем и не звонят гражданам с просьбами предоставить свои персональные данные и данные банковских карт;
- Сотрудник банка может запросить у клиента только контрольное слово и ФИО;
- При звонке сотрудник банка ни когда не попросит сообщить PIN код банковской карты.

### **ОМСКАЯ ПОЛИЦИЯ РЕКОМЕДУЕТ!!!**

**Если Вам поступил звонок от лица, представившегося сотрудником службы безопасности банка, либо иного представителя кредитно-финансового учреждения, в ходе которого предприняты попытки получения сведений о реквизитах карты и Ваших персональных данных, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в банк по официальному номеру контактного центра службы поддержки клиентов указанному на оборотной стороне банковской карты.**

**Если в отношении Вас и Ваших близких совершены мошеннические действия,  
незамедлительно обращайтесь в полицию!!!**

**ВСЕГДА НА СВЯЗИ 102**

*УМВД России по Омской области*

# ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ: ОСТОРОЖНО – МОШЕННИКИ!



- Вы получили СМС-сообщение о неожиданном выигрыше и Вам необходимо внести предоплату за его получение. Задумайтесь! Настоящий розыгрыш призов не должен подразумевать денежные выплаты с вашей стороны! Не торопитесь расставаться со своими деньгами!
- Вам звонят с незнакомого номера и тревожным голосом сообщают, что Ваши близкие попали в беду, а для того, чтобы им помочь, нужна крупная сумма денег. Не верьте! Обязательно позвоните родственникам, чтобы проверить полученную информацию.
- К Вам пришли незнакомые люди, представляющиеся работниками социальных и коммунальных служб, пенсионного фонда и т.д. и под любым предлогом просят пройти в дом. Прежде чем открывать входную дверь, позвоните в организацию, приславшую их. Мошенники занервничают, а настоящие работники отнесутся с пониманием. Никогда не отдавайте деньги, ценности и документы.
- К Вам пришли незнакомцы и предлагают купить лекарства, пищевые добавки и т.д. Знайте! Настоящие лекарства и пищевые добавки (БАД) следует приобретать только в аптеках и специализированных магазинах. А перед их употреблением нужно обязательно проконсультироваться с врачом.
- Если Вы пользуетесь банковскими картами и на Ваш мобильный телефон пришло подозрительное SMS – сообщение о том, что «Ваша банковская карта заблокирована», «Заявка на перевод 10.000 рублей Банком принята» и т.д. Не надо звонить по указанному в SMS-сообщении телефону, так как представившийся Вам специалист банка является мошенником. Не сообщайте свои Фамилию, имя, отчество, ПИН-код и номер банковской карты, а также цифры на обороте карты. Для решения возникших проблем необходимо обратиться в ближайшее отделение банка, либо позвонить в банк по телефону с федеральным номером, указанным на банковской карте 8 800 ....
- Если Вы разместили объявление или нашли интересующий Вас товар в сети Интернет, газетах, журналах и т.д. и Вам предлагают для его приобретения или продажи сообщить номер банковской карты – не верьте и не передавайте собеседнику эти данные!

**ПОМНИТЕ:** Если Вы или Ваши близкие стали жертвами мошенников, или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно звоните в полицию по телефону 02!

**Вам обязательно помогут!**