



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](http://fincult.info)



Финансовая  
культура





# КАК НЕ СТАТЬ ЖЕРТВОЙ **МОШЕННИКОВ**



## ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

**СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ  
БАНКОВ НИКОГДА НЕ ЗВОНЯТ  
КЛИЕНТАМ ДЛЯ ПРЕДУПРЕЖДЕНИЯ  
ОБ ИМЕЮЩИХСЯ ПРОБЛЕМАХ,  
СВЯЗАННЫХ С КАРТАМИ!**



**Не следуйте инструкциям звонивших и не отвечайте на задаваемые вопросы, а просто положите трубку!**



**Проверить информацию можно, позвонив в контактный колл-центр банка по телефону, указанному на задней стороне вашей банковской карты**

**Никогда и никому не сообщайте данные своей банковской карты (ПИН-код, код безопасности, пароли и др.)**

**Знайте, что мошенники уже могут располагать некоторой информацией о Ваших персональных данных!  
Будьте внимательны!**

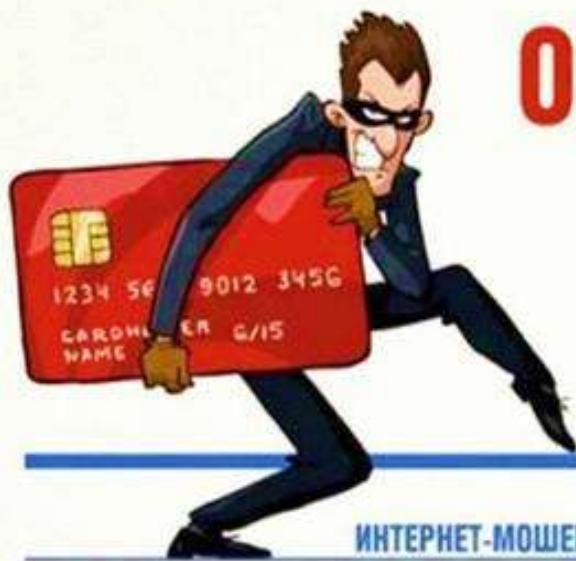


# ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Приморскому краю предупреждает, в регионе увеличивается количество случаев телефонного и интернет мошенничества.

-  1. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного- и интернет-банка, трехзначный код на обороте карты, коды из СМС.
-  2. Сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается якобы с официального номера банка, – дело рук мошенников!
-  3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните, все ли в порядке с вашими деньгами.
-  4. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.
-  5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.
-  6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!
-  7. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.
-  8. Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните! Попытка дать взятку – преступление!
-  9. В любой ситуации сохраняйте бдительность и критическое мышление! Не позволяйте мошенникам обманывать Вас!

Если вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону 02 или 102. Телефон Дежурной части Управления МВД России по Приморскому краю 8 (423) 249-04-91



# ОСТОРОЖНО: МОШЕННИКИ!

## НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

### ИНТЕРНЕТ-МОШЕННИКИ

#### ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

#### ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



#### СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страницей в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

### ТЕЛЕФОННЫЕ МОШЕННИКИ

#### ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

**Мама, я попал в аварию!**



#### БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

#### ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».



#### ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.





# Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

## Злоумышленники:

- Могут рассыпать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;
- Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;
- Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные;
- Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

## Следует помнить!

- Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не прсылают писем и не звонят гражданам с просьбами предоставить свои данные;
- Сотрудник банка может запросить у клиента только контрольное слово, ФИО;
- При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;
- Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;
- При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

## При несанкционированном (незаконном) списании денежных средств рекомендуется:

- Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;
- Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;
- Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону **02** (со стационарных телефонов) или **102** (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.