

# КУДА МОЖНО ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ ?

## В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ ПО МЕСТУ ЖИТЕЛЬСТВА:

соберите все документы, которые у вас есть:

- договоры, заключенные с посредником-мошенником;
- чеки на перевод денег;
- сделайте скриншоты с сайта и отправляйтесь в полицию писать заявление.



## ЗАДАТЬ ВОПРОС ПО ТЕЛЕФОНАМ:



**8-800-300-3000**

(бесплатно для звонков из регионов России)



**+7 (499) 300-3000**

(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

# ОСТОРОЖНО! МОШЕННИЧЕСТВО НА ФИНАНСОВОМ РЫНКЕ



## СЛУЖБА ПО ЗАЩИТЕ ПРАВ ПОТРЕБИТЕЛЕЙ И ОБЕСПЕЧЕНИЮ ДОСТУПНОСТИ ФИНАНСОВЫХ УСЛУГ БАНКА РОССИИ:



[fps@cbr.ru](mailto:fps@cbr.ru)



107016, Г. Москва,  
ул. Неглинная, д. 12



[www.cbr.ru](http://www.cbr.ru)

раздел «Сервисы. Интернет-приемная»

Материалы подготовлены в рамках реализации пункта 1.1.1(1) подпрограммы «Финансовое просвещение населения Краснодарского края» государственной программы Краснодарского края «Социально-экономическое и инновационное развитие Краснодарского края»

(постановление главы администрации (губернатора) Краснодарского края от 5 октября 2015 г. № 943)

Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете, вклады под невероятные проценты и онлайн-казино — все это виды финансового мошенничества. Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственных организаций, чтобы выманить деньги.

## КАК РАСПОЗНАТЬ МОШЕННИКА?

### ПРИЗНАК 1

#### НА ВАС ВЫХОДЯТ САМИ

Вам звонит незнакомец, присылает СМС-сообщение, электронное письмо или ссылку в мессенджере. Кем бы он ни представился — сотрудником банка, полиции, магазина, вашим троюродным братом-миллионером — насторожитесь. Раз он стал инициатором контакта, ему что-то от вас нужно.

Быстро проверить, тот ли он, за кого себя выдает, не получится. Номер, который высвечивается при входящем вызове можно подменить, аккаунты или сайты известных людей или организаций — подделывать. Так что стоит быть бдительным и никому не верить на слово.

### ПРИЗНАК 2

#### С ВАМИ ГОВОРЯТ О ДЕНЕГАХ

Основная задача мошенников — получить доступ к чужим деньгам. Схемы обмана почти всегда связаны с финансами: вам предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно» инвестировать свои сбережения (на самом деле — в финансовую пирамиду).

Легенды могут быть какими угодно, но речь всегда про деньги — которые вы можете потерять или получить.

### ПРИЗНАК 3

#### ВАС ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Если воров нужны ключи от квартиры, то финансовым мошенникам — «ключ» к деньгам на ваших счетах. Это могут быть конфиденциальные данные вашей карты, включая срок действия и три цифры с ее обратной стороны. Либо логины и пароли к личному кабинету на сайте банка или мобильному приложению. И почти всегда — коды



из банковских уведомлений

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

Когда банк замечает сомнительный платеж или перевод с вашего счета, с вами связываются, чтобы подтвердить или отклонить операцию, и только. Конфиденциальные данные для этого не требуются. Если о них спрашивают — будьте уверены, звонят не из банка и вас точно попытаются обмануть.

### ПРИЗНАК 4

#### ВАС ВЫВОДЯТ ИЗ РАВНОВЕСИЯ

Мошенники стремятся вызвать у вас сильные эмоции — напугать или обрадовать. Так они сбивают с толку и притупляют бдительность потенциальной жертвы. Например, сообщают: «ваш онлайн-банк взломали!», чтобы вы от растерянности и волнения выполнили любые просьбы и выдали любую информацию, лишь бы спасти деньги.

Либо, наоборот, огорчивают новостью о внезапном выигрыше в лотерею или обещают быстрее обогащение. Взамен вы должны будете «лишь оплатить небольшой взнос», а для этого — ввести данные банковской карты на сайте. Мошенники создают фишинговые страницы, с помощью которых воруют данные карт и получают доступ к банковским счетам доверчивых пользователей.

### ПРИЗНАК 5

#### НА ВАС ДАВЯТ

Мошенники всегда торопят, чтобы не дать вам времени обдумать ситуацию. Вас принуждают к чему-то, ставят условия: «сейчас или будет поздно». Ситуация, в которой вам не дают права выбора и заставляют немедленно действовать, подозрительна.

Если чувствуете психологический дискомфорт, лучше сразу же прекращайте общение. Ведь чем дольше вы разговариваете с мошенником, тем сильнее он будет на вас давить. На все ваши расспросы у обманщиков есть заготовленные ответы, которые только нагнетают обстановку.

## СОВЕТЫ, КОТОРЫЕ ПОМОГУТ НЕ СТАТЬ ЖЕРТВОЙ ФИНАНСОВЫХ МОШЕННИКОВ:



1. Никогда не принимайте поспешных решений, особенно если они касаются ваших финансов. Всегда берите паузу, чтобы разобраться в том, что происходит. Возьмите за правило перепроверять любую информацию в первоисточнике.
2. Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить

реальное положение дел.

3. Пришлили странное уведомление от имени Федеральной налоговой службы (ФНС)? Заверьте личный кабинет на сайте ФНС — в нем можно проверить суммы налогов и сразу же оплатить их.

4. Получили «письмо счастья» о государственной выплате? Помогите новости об этом в деловых СМИ. А еще лучше — найдите сам закон, указ или постановление, которые вводят выплаты. Обратите внимание на условия, кому они положены.

5. Не перечисляйте деньги на счета незнакомцев ни под каким предлогом. Мошенники могут сообщить о выигрыше в лотерею, о компенсации затрат, о возврате налогов и прочее. Однако для получения приза, например, необходимо перечислить определенную сумму.

6. Не переводите денежные средства на счета мобильных телефонов, на электронные кошельки. Причем даже в случае, если вас просят сделать это при совершении покупки. Подавляющее число интернет-магазинов принимают оплату по факту доставки товара. Так лучше воспользоваться этим надежным способом расчета.

7. Не отправляйте ответных сообщений на незнакомые номера (особенно на короткие) и не перезванивайте. И, тем более, не отправляйте деньги ни на какие реквизиты, указанные в сообщении. Даже если оно написано от имени банка или госструктуры, лучше уточнить информацию, позвонив на официальный номер учреждения.

8. Приобретая товары с рук на условиях предоплаты, убедитесь в благонадежности Продавца. Посмотрите отзывы, узнайте его рейтинг на площадке объявлений, да и в целом поищите какую-нибудь информацию в информационно-телекоммуникационной сети «Интернет».

9. Не сообщайте никому данные своей банковской карточки. В особенности это касается кода СМС и CVV2, расположенного на оборотной стороне. Также не озвучивайте кодов из СМС, отправляемых банком и, тем более, ни в коем случае не сообщайте никаких паролей.

10. Не переходите по ссылкам, присланным с незнакомых номеров.

11. Перед снятием денег в банкомате осмотрите его. На картпримемнике не должно быть посторонних предметов, клавиатура не должна шататься.

12. Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.

13. Подключите мобильный банк и СМС-уведомления.

14. Старайтесь никогда не терять из виду вашу карту.

**Не всегда при общении с аферистом вы заметите все признаки мошенничества. Но в любой ситуации стоит проявлять бдительность.**