



## Кибермошенничество

Допустим, вы всегда снимаете деньги только в кассе банка, а картой и вовсе не рассчитываетесь. Вы чувствуете себя в безопасности. Вдруг вам приходит СМС или письмо якобы от банка со ссылкой, просьбой перезвонить по неизвестному номеру или с уведомлением о неожиданном крупном выигрыше. Или звонят от имени банка и просят сообщить личные данные, ПИН-код от карты или номер СМС-подтверждения. Или пишут в социальных сетях от имени родственников или друзей, которые внезапно попали в беду (угодили в полицию, сбила машина, украли сумку) и просят перевести определенную сумму денег на неизвестный счет.

В 99,9% случаев вы имеете дело с мошенниками. За ссылками, скорее всего, таятся вирусы, на другом конце провода — специалисты по обману, которые всеми правдами и неправдами хотят выманить необходимые им данные, а по ту сторону экрана — злоумышленники, которые играют на ваших желаниях, чувствах и заботе о близких.

### Как не попасться

- Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.
- Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС — не от вашего банка, а звонил вам злоумышленник. Проверьте

состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

- Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.
- Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам.
- Не храните данные карт на компьютере или в смартфоне.
- Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты.
- Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.
- Установите на компьютер антивирус — и себе, и родственникам.
- Объясните пожилым родственникам и подросткам эти простые правила.

**Видов кибермошенничества много, для каждого случая - свой вариант решения**

**Меня обманули. Что делать?**

- Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.
- Обратитесь с заявлением в отдел полиции по месту жительства или отправьте обращение в управление «К» МВД России.

По материалам сайта <http://fincult.info/articles/moshennichestvo-na-finansovom-rynke/how-to-protect-yourself-and-loved-ones-from-financial-fraud/>