Как уберечь себя и близких от финансового мошенничества

Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете и вклады под невероятные проценты, онлайн-казино — все это виды финансового мошенничества. Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственные организации, чтобы выманить деньги. Как распознать мошенника и что делать, если вас все-таки удалось обмануть?



Стать жертвой преступников может каждый, и неважно, использует он банковскую карту или предпочитает рассчитываться наличными. Мошенники умеют выманивать деньги онлайн, с помощью звонков и СМС, в социальных сетях и офисах. Как они это делают?

**Мошенничество с банковскими картами**

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.



**Номер CVC или CVV — три цифры, расположенные на поле для подписи владельца карты или рядом с ним.**

[**Подробнее о том, как устроена банковская карта**](https://fincult.info/article/kak-ustroena-bankovskaya-karta1/)**.**

Достаточно один раз воспользоваться таким банкоматом и не прикрыть рукой клавиатуру в момент набора ПИН-кода — и ваши деньги могут снять, перевести на несколько счетов и обналичить. Украсть данные вашей карты могут даже в кафе или магазине. Злоумышленником может оказаться продавец, который получит доступ к вашей карте хотя бы на пять секунд. Сфотографировав вашу карту, он сможет воспользоваться ей для расчетов в интернете.

**Как не попасться**



* Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
* Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
* Подключите мобильный банк и СМС-уведомления.
* Если совершаете покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит вам по СМС.
* Старайтесь никогда не терять из виду вашу карту.

**Меня обокрали. Что делать?**

1. Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.
2. Запросите выписку по счету и напишите заявление о несогласии с операцией.
3. Обратитесь с заявлением в отдел полиции по месту жительства или [отправьте обращение](https://xn--b1aew.xn--p1ai/request_main) в управление «К» МВД России.

**Подробнее о том, как**[**злоумышленники могут украсть ваши деньги в повседневной жизни**](https://fincult.info/article/kto-i-kak-okhotitsya-za-vashimi-kartami/)

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 энную 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 c 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**](https://fincult.info/article/kto-i-kak-okhotitsya-za-vashimi-kartami/)

**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](https://xn--b1aew.xn--p1ai/request_main) в управление «К» МВД России.