

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Мошенничество с банковскими картами тоже распространенный способ жульничества. Выделяют три основных вида такого мошенничества.

Обычная кража. Зачастую это происходит из-за неаккуратности самих владельцев карт, которые выкладывают их фотографии в социальных сетях. Здесь рецепт прост: берегите свою карту, никому не сообщайте информацию о ней, а в случае кражи сразу же звоните в банк и блокируйте карту.

Мошенничество через телефон или Интернет. Вам может поступить звонок от человека, который представится сотрудником банка. Под разными предлогами — от специального предложения до обеспечения сохранности ваших средств — мошенник будет стараться узнать данные вашей карты, после чего выведет с нее все средства. Помните, что у банка есть вся необходимая информация о вашей карте, не сообщайте о ней ничего по телефону.

Мошенничество через банкоматы. Иногда преступники встраивают в банкоматы специальные считывающие устройства, которые позволяют скопировать всю информацию о вставленной карте. Единственный способ защититься от такого вида мошенничества — не использовать банкоматы, где эти сканеры могут стоять.

Перед использованием банкомата оцените, насколько крепко к нему приделана та часть, в которую вставляется карта, а также клавиатура. Если они слабо держатся, лучше этим банкоматом не пользоваться. Кроме того, не стоит пользоваться банкоматами, расположенными в сомнительных, безлюдных местах; лучше снять деньги в офисе банка или в государственном учреждении, там банкоматы со сканером встречаются крайне редко.

Как защитить свою карту?

Чтобы защитить себя от мошенников, нужно следовать простым правилам:

1. Подписывайте свои карты. Многие забывают расписаться на оборотной стороне карты, а ведь эта подпись может быть полезной для установления ее владельца.
2. Никому (даже сотрудникам банка!) не сообщайте конфиденциальную информацию о своей карте: пин-код, CVV-код, логин и пароль от личного кабинета онлайн-банка.

Если вы подозреваете, что кто-то мог узнать эти данные, поменяйте их.

3. Настройте информирование обо всех операциях по картам. Самый быстрый и надежный способ — через СМС, но можно настроить также пуш-уведомления в смартфонах и по электронной почте. Это позволяет быстро узнать, что кто-то получил доступ к вашему счету.
4. Установите лимит по снятию денег с карты. Такой способ защиты карты не защитит от взлома, но снизит потери от него.
5. Не печатайте чек в банкомате, если это возможно. Данные о вашей карте представлены в этом чеке. Если он вам не нужен, не печатайте его, так надежнее. Если банкомат все же печатает чек, уничтожьте его, чтобы чек нельзя было восстановить и по нему вычислить данные вашей карты.
6. Не отдавайте вашу карту никому (!), даже официантам. Требуйте, чтобы продавец или официант использовал терминал для оплаты покупки или счета при вас. Убедитесь в том, что сумма, указанная в терминале, совпадает с тем, сколько вы должны заплатить.
7. Закрывайте клавиатуру банкомата при вводе данных. Не бойтесь показаться параноиком! Этот простой прием защитит вас от камер, которые могли поставить злоумышленники, чтобы узнавать пин-коды чужих карт.
8. Не используйте свою карту на неизвестных и ненадежных сайтах. Для покупок в Интернете лучше завести специальную виртуальную карту, на которой будет храниться небольшая сумма денег.
9. Если у вас произошла неприятность, сразу же звоните в банк, пока мошенники не успели списать деньги.

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.



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.