Банковская карта и безопасность

Пользуйтесь банковскими картами безопасно

С каждым годом людей, активно использующих банковские карты, становится все больше. И как следствие, так же стремительно растёт количество обманных действий с ними. Настораживает, что в большинстве случаев люди сами называют мошенникам PIN-коды, номера карт и одноразовые пароли. Помните, что это делать категорически нельзя. А как еще можно обезопасить свои финансы, читайте далее.

Простые правила

- Никогда и никому не сообщайте данные карты и пароли из пришедших SMS, если вам позвонили неизвестные. Даже если они представляются сотрудниками вашего банка, Центрального банка РФ, да кем угодно. Молчите, как партизан, и прекращайте разговор.

  Банк никогда не обратится к вам с просьбой предоставить конфиденциальную информацию, такую как PIN-код и CVV2/CVC2. В случае получения подобного запроса – немедленно сообщайте об этом в ваш банк.

- Подключайте SMS-оповещение об операциях. В случае получения сообщения о покупке, которая не была совершена, блокируйте карту. Это всегда можно сделать через интернет-банк или обратившись в call-центр банка. При этом блокируется карта, а не счет, к которому она привязана.

  Устное заявление об утрате карты должно быть обязательно подтверждено подачей в банк письменного заявления на блокировку карты в течение 72 часов.

- Чтобы минимизировать потери при попадании карты в чужие руки, устанавливайте лимиты на снятие средств.
- Помните, банк не свяжется с вами через популярные мессенджеры, такие как Viber или WhatsApp. Если вы получили такое сообщение, позвоните в свой банк.
- При оплате картой покупок не выпускайте ее из виду и не передавайте ее третьим лицам.
- При снятии средств в банкомате (ровно как и при оплате в магазине) прикрывайте панель ввода ладонью.
- Если для доступа к банкомату необходимо использовать картридер (располагается рядом с дверью) лучше для этого использовать какую-нибудь другую банковскую карту.

Не ставьте все на карту

Не держите все ваши деньги на одной карте. Заведите себе дополнительную с кешбэком и с ней ходите в магазин с конкретной суммой денег. А лучше держите все деньги на вкладе с возможностью снятия без потери процентов и с него через интернет-банк переводите средства на карту, которой рассчитываетесь.

Также помните, что свою карту нельзя давать использовать кому-то другому. Это считается грубым нарушением правил в каждом банке. Поэтому для своих близких лучше выпустить дополнительные карты. Тем более что даже в случае блокировки основной они продолжают действовать до окончания своих сроков.

Для покупок в интернете – отдельная карта

С развитием онлайн-шопинга мошенники активизировались и в сети. Чаще всего злоумышленники пытаются украсть данные банковских карт.

- С помощью поддельных сайтов, внешне очень похожих на оригинальные (фишинг).
- Программ загрузки, если пользователь что-то качает в интернете из непроверенных источников.
- В письмах на электронной почте с обещанием «большого наследства от умершего дядюшки».
- С помощью дубликатов SIM-карт, получая доступ к одноразовым паролям для подтверждения оплаты.

Следует соблюдать правила безопасности в интернете: использовать хороший антивирус, проверять правильность написания сайта (нет ли в нем лишних символов), не верить в «бесплатный сыр» и, конечно, периодически менять пароли для входа в интернет-банк и от аккаунтов в соцсетях и онлайн-магазинов. Но самое главное – **разделить траты в сети и траты в обычных магазинах: для онлайн-шопинга используйте отдельную карту**.

Раньше большой популярностью у клиентов банков пользовались так называемые виртуальные карты. Они выпускались на короткий срок с определенной суммой денег, и на сайте для покупки можно было вводить ее данные, а не данные основной карты. Но со временем спрос на них упал, и сейчас найти банк, предоставляющий такую услугу, довольно сложно. Это связано с тем, что сами банки стали пристальнее следить за безопасностью покупок своих клиентов в сети.

Сейчас на большинстве сайтов подтверждение покупки совершается через технологию 3D-secure – одноразовые пароли, которые приходят владельцу карты на телефон.

Впрочем, есть и исключения. Так, популярный ресурс Aliexpress не требует ввода одноразового пароля. Поэтому на всякий случай лучше иметь отдельную карту для покупок в интернете с установленным на ней лимитом трат в сети.

Бесконтактные платежи – могут ли украсть?

После выхода на рынок банковских карт с возможностью бесконтактных платежей появились разного рода «страшилки» о том, что с них можно легко умыкнуть деньги. В действительности системы оплаты в одно касание достаточно хорошо защищены. Для злоумышленника способ хищения денег с карты может оказаться крайне невыгодным и весьма проблематичным в осуществлении. Поэтому не стоит опасаться карт с бесконтактным способом оплаты. А лучше и надежнее использовать для покупок смартфон, если конечно он такой функцией обладает.

Какую информацию могут запрашивать сотрудники банка?

Если вы сами позвонили в банк, например, узнать о статусе готовности карты, то операционист может задать вам несколько вопросов, чтобы вас идентифицировать. Чаще всего просят назвать последние две цифры паспорта, или номер телефона, или дату рождения. Если вы клиент банка, то могут запросить ваше кодовое слово. Если же вам позвонили, представились сотрудником банка и просят назвать ваши персональные данные, сразу прекращайте разговор и позвоните по номеру call-центра банка для уточнения обстоятельств – возможно, вас пытаются обмануть.