КАК ЗАЩИТИТЬСЯ ОТ «СКИММИНГА»?

Банковская платежная карта является персонифицированным платежным средством и позволяет ее законному держателю производить оплату товаров, услуг. Использование компьютерных технологий в сфере платежей, покупок, в кредитовании является характерной чертой повседневной жизни. Помимо множества удобств и достоинств, электронные платежные средства имеют и оборотную сторону.

Мошенничество с банковскими картами развивается вместе с развитием банковских технологий. Постоянно растет количество преступлений, связанных с преступлениями в сфере информационных технологий. Новые технологии открывают мошенникам доступ к электронным счетам владельцев финансовых средств. Повсеместное использование карт для выплат заработной платы, расчетов в магазинах, получения кредитов привлекает разного рода мошенников, которые постоянно находят новые способы добычи информации о кредитных картах и несанкционированного снятия денежных средств.

Мошенничество с банковскими картами подразумевает использование данных вашей пластиковой карты для проведения операций без вашего ведома. В зависимости от данных вашей карты, которые оказались в руках мошенников, возможны различные незаконные операции с карт-счетом:

- если карта просто украдена, но не заблокирована, мошенник может осуществить покупку в магазине, сымитировав вашу подпись, образец которой есть на карте. Если есть карта и ПИН-код, то с карты можно снять все денежные средства, если на карту открыт овердрафт, мошенник может снять и деньги по кредитному лимиту.
- перехват пластиковой карты, выпущенной и пересылаемой владельцу по почте. Кража обнаруживается с большим опозданием, в результате отсутствует возможность немедленного блокирования счета; к моменту кражи карточки, как правило, не подписаны, а значит, злоумышленник может поставить свою подпись и легально использовать карточку по своему усмотрению. Выявлены случаи, когда преступники специально устраивались работать на почту или в частные службы доставки, чтобы иметь возможность изымать конверты с пластиковыми банковскими карточками.
- двойная прокатка карты через терминалы в магазине. Прокатка карты осуществляется для оплаты, для снятия копии реквизитов карты. Двойная прокатка карты может привести к двойному снятию денег за оказанную услугу либо покупку.
- Мошенничество с использованием минимальных сумм покупки по карте. Фальшивые карты мошенники используют в туристических поездках, делая вдали от своей страны покупки на небольшие суммы. При таких суммах покупки терминалы магазинов не производят авторизацию счета карты (терминал не связывается с банком для проверки счета). При покупке считывается только СЛИП карты. СЛИП передается в банк с небольшой

задержкой по времени, также с задержкой по времени обновляется СТОП-ЛИСТ банка. Используя задержки в обработке платежей, мошенник может сделать покупки на внушительные суммы.

Во избежание хищения денежных средств рекомендуется следующее.

1)Не верьте звонкам из «банка». Во-первых, знайте, что сотрудники банка и так все о вас знают. Максимум, что они могут у вас спросить, - кодовое слово. Да и то лишь в том случае, если вы сами им позвонили, а не наоборот. Во-вторых, попросите «сотрудника» набрать вам через пять минут или положите трубку. А сами в это время позвоните по номеру, который указан на вашей карте, и поговорите с реальной службой поддержки банка. Самое главное правило: НИКОГДА И НИКОМУ НЕЛЬЗЯ СООБЩАТЬ полные данные своих банковских карт, CVV-код и одноразовые пароли, приходящие по СМС».

2) Отключите всплывающие окна. Если заполучить карту и телефон человека, то можно и ПИН-код поменять, и совершать любые транзакции. Суть в том, что на большинстве смартфонов уведомления приходят прямо на экран. Необходимо отключить на своем телефоне всплывающие окна. Тогда посмотреть полученные сообщения можно будет только после разблокировки. Эту функцию можно настроить на любом смартфоне.

3) Используйте виртуальную карту. Мошенникам ничего не мешает создать фиктивный сайт с очень привлекательными ценами, чтобы заполучить данные тысяч банковских карт. А дальше - дело техники. До сих пор во многих онлайн-магазинах, чтобы совершить покупку, вводить код из СМС не нужно, и это открывает простор для деятельности мошенников. Главное - заполучить данные с обеих сторон банковской карты.

Банки всегда советуют не показывать никому оборотную сторону карты и секретный код, который написан на ней. Но уберечь карту от чужих глаз не всегда получается. В отличие от ПИН-кода эти три цифры напечатаны прямо на карте. Украл пластик - и вперед. Эксперты советуют хотя бы для покупок в интернете использовать виртуальную карту. Ее можно создать в мобильном приложении. Такую услугу предлагают многие крупные банки. Переводите на виртуальную карту нужную сумму - и совершаете покупку в интернете. Это уменьшит то время, когда вы пользуетесь реальной картой, таким образом, у мошенников будет меньше возможностей узнать данные вашей реальной карты и соответственно ими воспользоваться.

4) Установите лимит по снятию наличных. Этот способ применяется все реже, но операции со снятием наличных все же лучше минимизировать. Если мошенник ввел правильные цифры ПИН-кода на клавиатуре, доказать, что деньги в банкомате снимали не вы, практически невозможно.

Если вам не нужны крупные суммы в купюрах каждый день, установите минимальный дневной лимит на снятие наличных - это крупная сумма, которой могут поживиться мошенники. Если большой объем наличных потребуется вам самому, увеличить дневной лимит можно либо в мобильном приложении, либо через кол-центр банка. А потом снова опустить до безопасного уровня.

5) Держите сбережения на резервном счете. Если мошенник украл у вас карту, значит, он получил ключ от вашего счета. Чтобы избежать этого, то необходимо заблокировать карту, но можно и не успеть это сделать.

Счетов в банке у вас может быть несколько, карта обычно привязана только к одному. Но на нем обычно лежат все деньги. Это неправильно. Основные средства лучше держать на том счете, который не привязан к карте. Если не хватает, можно прямо перед покупкой сделать перевод между своими счетами. В мобильном приложении это можно сделать за несколько секунд. И счет лучше пусть будет накопительный - заодно и проценты набегут.

Можно ли вернуть украденные с карты деньги?

По закону «О национальной платежной системе» (статья 9) банк обязан вернуть клиенту деньги, но с некоторыми оговорками. Во-первых, мошенники должны списать их без ведома владельца карты. Во-вторых, операцию нужно оспорить не позднее следующего дня с момента получения от банка уведомления о списании средств. Тем не менее, на практике в большинстве случаев человек сам сообщает мошенникам ПИН-код, CVC/CVV (код из трех цифр с обратной стороны карты), в связи с чем считается, что он добровольно дал согласие на перевод денег и банк отказывается возмещать потери.

Вместе с тем, необходимо незамедлительно сообщить о правонарушении в банк, одновременно обратившись в правоохранительные органы.