Как действуют мошенники и как себя уберечь

ответ UrOpora.ru

1. Наиболее распространенное мошенничество с банковской картой – это заклеивание той части, из которой пользователь получает деньги. Принцип очень простой: человек приходит снимать деньги с пластиковой карточки, вводит секретный код, сумму, а деньги свои получить не может. Естественно, что некоторое время он возмущается, а через полчаса идет домой в расстроенных чувствах и с желанием завтра с утра разобраться с нерадивыми банковскими работниками. После ухода человека, выходит злоумышленник, отклеивает скотч, которым было заклеено отверстие и забирает деньги. Стоит отметить, что работает такой способ только в темное время суток. Чтобы не попасть в подобную неприятную ситуацию, старайтесь снимать деньги днем, а если вы не можете получить деньги, внимательно осмотрите внешнюю сторону банкомата на наличие лишних элементов (скотча, например). Если все в порядке, а денег по-прежнему нет, обратитесь в службу банка.
2. Мошенничество оффлайн. Сюда можно также отнести грабеж денег сразу же после их снятия. Кроме этого, недобросовестные сотрудники магазина или кафе могут провести вашу карточку через кардридер два раза, в итоге вы заплатите два раза. Чтобы быть в курсе всех ситуаций, которые происходят с пластиковой картой, подключите услугу информирования посредством смс. Карточка, которую

потеряли, но не заблокировали, также может стать объектом несанкционированного вмешательства мошенников. Еще одно достаточно простое мошенничество с пластиковыми картами – попробовать оплатить какой-то товар найденной пластиковой карточкой. Естественно, чтобы избежать таких ситуаций, следует после утери сразу же обращаться в банк. И получать новую карту лучше не по почте, а придя лично в банк. Письма с новыми картами иногда перехватывают недоброжелатели.

3. Еще одно мошенничество с банковскими картами – фишинг. Вам звонят на телефон или же приходит письмо на электронный ящик, где под любым предлогом просят сказать или написать данные вашей карты. Это может быть какая-то акция, которая нацелена на предотвращение несанкционированных транзакций. Будьте внимательны и не слишком доверчивы, запомните, что никто не имеет права узнавать у вас такую личную информацию, тем более посредством телефона или почты. Даже работникам банка вы не должны сообщать свой пин-код. И старайтесь его нигде не записывать, а хранить в памяти.
4. Фишинг неэлектронный. Данное мошенничество с картами банка связано с приобретением товаров и оплатой за них карточкой, с обязательным вводом владельцем пин-кода. Когда владелец карты расплачивается за свои покупки, услуги или же наоборот, снимает свои деньги, ему не обязательно снимать деньги с карты, а только после этого отдавать их продавцу. Для этого применяют специальные микропроцессорные карты. Как действуют мошенники – они копируют с магнитных полос лент данные и одновременно записывают персональный идентификационный номер человека. После этого они по полученным данным создают новую поддельную карточку, по которой снимают деньги в банкоматах города со счета ее истинного владельца. Тяжело обезопасить себя от такого жульничества, однако мы можем порекомендовать, не использовать пластиковые карты в сомнительных торговых точках.
5. Неправомерные действия в интернете. Вы можете очень

просто лишиться всех своих средств, если вы осуществляете какие-либо платежи через интернет. У мошенников есть возможность перехватить деньги прямо во время оплаты. Поэтому, мы не советуем делать какие-либо крупные покупки через интернет, несмотря на то, что это очень удобно, и к тому же, очень популярно. Особенно это касается незнакомых сайтов, лучше используйте в таких случаях виртуальной карточкой. На ней, как правило, можно установить определенный лимит средств, и злоумышленники не смогут украсть больше этого лимита. Рекомендуется подключить свою карту к специальной услуге, благодаря которой для произведения любой операции в интернете с картой, вы должны будете ввести присланный смс сообщением код. Так ваши денежные средства будет тяжелее украсть. Если вы не знаете или плохо знаете иностранный язык, лучше воздержитесь от электронных покупок и оплат своей картой на иностранных сайтах.

6. Скимминг. Это еще одно мошенничество с платежными картами, которое становится очень распространенным. На банкоматах и платежных терминалах устанавливают такие устройства, как скиммеры. Они считывают данные с карточки, а после на их основании мошенники выпускают дубликаты пластиковых карточек и по ним снимают деньги, применяют там, где не нужно подтверждение личности. Чтобы отследить мошенников, старайтесь очень тщательно контролировать свои расходы, чтобы быть уверенным в том, что только вы один снимаете деньги со своего счета.
7. Еще один метод – узнать пин-код и также несанкционированно снимать деньги. Узнать его можно многими способами, среди которых: подсмотреть в то время, когда владелец его набирает, нанести особый клей, на котором четко видно набранные цифры, установить небольшую камеру на банкомате. Будьте внимательны, не позволяйте прохожим смотреть на клавиатуру и дисплей банкомата, когда вы снимаете там деньги. Кроме этого, лучше воздержитесь от снятия денег в темное время

суток в незнакомом районе, особенно в то время, когда улицы уже пусты.

8. Вирус, который действует на банкоматы. Это – один из самых новых способов мошенничества, он еще не успел набрать широкого распространения, особенно в нашей стране. Вирус не только следит за всеми операциями, которые происходят на банкомате, но и передает ценную информацию мошенникам. Однако не переживайте о том, что можете стать жертвой такого обмана. Как говорят специалисты, написать подобную программу достаточно сложно, для этого мошенникам нужно применять необычную операционную систему и при этом общаться с банками по достаточно защищенным системам.
9. Чтобы обезопасить себя от неприятных ситуаций, связанных с мошенничеством, рекомендуем обратить внимание, какая у вас пластиковая карта – с чипом или магнитная. Чиповые карты более защищены от взломов, подделок и т.д. Мошенникам тяжело осуществить свои зловещие планы из-за того, что данные на обычной карточке уже нанесены на магнитную полосу, а на чиповой – при каждой операции банкомат и карта обменивается данными. Любой владелец пластиковой карты банка должен осознавать, что всегда существует очень большой риск того, что именно он станет одной из жертв обмана и попадет в сети мошенников. Однако, если внимательно ознакомиться с главными приемами преступников, то риск того, что вы попадете в неприятную ситуацию, будет гораздо ниже. Ведь кто предупрежден – тот вооружен.