Современный человек все больше покупок делает с помощью пластиковой карты, которая уже давно стала частью нашей жизни. Мы покупаем билеты на самолет, оплачиваем счета, не выходя из дома, расплачиваемся за продукты в супермаркете и кафе одним движением. Управление Роспотребнадзора по Республике Алтай напоминает, что для сегмента банковских карт в современных условиях характерен ряд рисков, которые вызваны стремительным развитием карточного мошенничества.

Наиболее распространенными схемами мошенничества с банковскими картами являются следующие:

- **оглашение сведений о ПИН-коде самим держателем карты.** Имеется ввиду, к примеру, запись ПИН-кода на карте или каком-либо носителе (лист бумаги, записная книжка, мобильный телефон), хранимом вместе с картой. Соответственно, если карта утеряна или украдена (вместе с сумкой, бумажником), у мошенника оказывается и карта и персональный код;

- **использование в своих целях карты с предварительной осведомленностью о ПИН-коде людьми, имеющими доступ к месту хранения карты.** Мошенник вполне может узнать ПИН-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит код в банкомате. Затем злоумышленник осуществляет кражу карты и использует ее в своих целях;

- **«Ливанская петля».** Как вариант подглядывания из-за плеча. Пока владелец карточки погружает ее в банкомат, она застревает. В это время подходит «советчик», который рекомендует срочно идти и звонить в сервисную службу, к примеру. Владелец карты уходит, а тем временем «советчик», видевший как он набирал ПИН-код, вытаскивает карту и снимает деньги;
- **фальшивые банкоматы.** Мошенники разрабатывают и производят фальшивые банкоматы, либо переделывают старые, которые выглядят как настоящие. Размещаются банкоматы в наиболее оживленных местах. После введения карты и ПИН-кода обычно на дисплее фальшивого банкомата появляется надпись, что денег в банкомате нет или, что банкомат не исправен. К тому времени мошенники уже скопировали с магнитной полосы карты информацию о счете данного лица и его персональный идентификационный номер;
- **копирование магнитной полосы (skimming).** Данный вид мошенничества предусматривает использование особых видов устройств, считывающих информацию с магнитных полос карт. Обычно это специально изготовленные клавиатуры, которыми накрывают существующие. Законный держатель банковской карты проводит операцию с вводом персонального идентификационного номера (ПИН), в это время, дополнительно установленное устройство считывает и записывает информацию на магнитной полосе, т.е. у злоумышленников появляются данные необходимые для дальнейшего

изготовления поддельной карты и ее использования в своих целях;

- **ложный ПИН-ПАД.** Держателю карты может быть предложено ввести ПИН-код не в настоящий ПИН-ПАД (устройство для ввода ПИН-кода), а в его имитацию, которая запомнит введенный код. Такие ложные устройства иногда устанавливают рядом со считывающими датчиками, предназначенными для прохода в помещение с банкоматом с использованием в качестве идентификатора (электронного ключа) банковской карты;

- **ограбление держателей банковских карт.** Самый незамысловатый способ. Клиент снял наличность - жулик ограбил;
- **фишинг (от англ. fishing).** В вольном переводе «закидывание удочки». Термин появился для обозначения новых схем, в результате которых путем обмана становятся доступны реквизиты банковской карты и ПИН-код. Чаще всего используется в виде рассылки через Интернет писем от имени банка или платежной системы с просьбой подтвердить указанную конфиденциальную информацию на сайте организации

- **вишинг (англ. vishing)** – новый вид мошенничества – голосовой фишинг, использующий технологию, позволяющую автоматически собирать информацию, такую как номера карт и счетов;
- **неэлектронный фишинг.** Данный вид связан с осуществлением покупок в торговых организациях посредством обязательного ввода ПИН-кода. В схемах неэлектронного фишинга создаются реальные торгово-сервисные предприятия/офисы банков, либо используются уже существующие. Держатели платежных карт совершают покупки товаров, получают услуги либо снимают денежные средства в кассе банка. Операции производятся с использованием банковских микропроцессорных карт и сопровождаются введением клиентом своего ПИН-кода. Сотрудники мошеннических предприятий негласно копируют информацию с магнитной полосы карты и производят запись персонального идентификационного номера. Далее мошенники изготавливают поддельную банковскую карту, и в банкоматах производится снятие денежных средств со счета клиента.

Меры безопасности при пользовании банковскими картами

Запомнить ПИН-код — это самый банальный совет, который можно дать пользователю пластиковой карты. Но люди продолжают хранить ПИН-код рядом с картой в кошельке или в открытых доступных местах, писать его на бумажках. Так делать нельзя. Запомнить код можно, привязав в памяти цифры к чему-то значимому для вас. Если запомнить никак не получается, запишите код в телефонной книге, назвав его каким-нибудь именем.

Всегда прикрывайте кнопки в процессе введения ПИН-кода рукой.

Не показывайте никому CVC2-код (это трехзначная комбинация на обратной стороне карты) и не отдавайте карту работнику магазина или кафе, если он предложит провести операцию без вашего участия.

Использовать мобильное приложение банка удобно и просто — вы можете совершать операции, контролировать расходы, да и безопасность у таких приложений хорошая. Однако даже в этом случае появляется риск: если вы открываете мобильный или интернет-банк, подключившись к непроверенной точке Wi-Fi (например в кафе), то рискуете стать жертвой мошенников. Старайтесь пользоваться мобильным приложением только тогда, когда ваш гаджет подключен к проверенной сети.

Обязательно используйте SMS-уведомления. Некоторые пользователи банковских карт считают дополнительные платные услуги лишними, пусть даже это и стоит меньше 100 рублей в месяц. Однако если с вашего счета станут исчезать деньги и вы не будете об этом знать, то можете потерять гораздо больше. SMS-уведомления позволяют всегда быть в курсе манипуляций с картой. Если вам неожиданно придет сообщение о снятии средств, вы сможете оперативно позвонить в банк и заблокировать карту. Часто мошенники не имеют возможности снять все средства сразу, в таких ситуациях каждая секунда на счету. Ведь даже если у вас украли карту, то это не значит, что у вас украли деньги на карте. Карту можно оперативно заблокировать, позвонив по бесплатному телефону в банк 24 часа в сутки и 7 дней в неделю.

Всех описанных выше неприятностей можно легко избежать, если придерживаться золотого правила: никогда, никому и ни под каким предлогом не сообщать реквизиты банковской карты. Помните, ни один работник банка не попросит клиента сообщить ему коды, пароли и прочие подобные данные. Получая какие-либо уведомления от банка в виде SMS или по e-mail, с просьбами связаться с банком или предоставить данные своей карты, не отвечайте и не перезванивайте по телефонам, указанным в этих сообщениях, используйте контакты, указанные на обратной стороне карты или на официальном сайте банка. Специалисты банков делают все от них зависящее, чтобы обезопасить карты и счета своих клиентов.

В случае утери или компрометации карты необходимо немедленно блокировать карту и связаться со специалистами. Обеспечить безопасность банковских карт и

интернет-банкинга не так сложно, нужно лишь установить для себя ряд разумных правил поведения и никогда от них не отступать.