# СПОСОБЫ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

**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.

**Дружественное мошенничество.** Использование в своих целях карты с предварительной осведомленностью о ПИН-коде членами семьи, близкими друзьями, коллегами по работе. То есть людьми, имеющими доступ к месту хранения карты.

**Подглядывание из-за плеча**. 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. Для его применения используется небольшой отрезок фотопленки, который складывается пополам, а края загибаются под углом в 90 градусов. Это приспособление вставляется в банкомат. «Изюминкой» является вырезанный на нижней стороне фотопленки на определенном расстоянии от края небольшой лепесток, отогнутый вверх по ходу карты. Пленка располагается в картридере так, чтобы не мешать проведению транзакции. Отогнувшийся лепесток не позволяет банкомату выдать пластиковую карту обратно. То есть, совершив операцию, владелец карты не может получить её обратно из банкомата. 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 устанавливают 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 появляется 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. Phishing).** Схемы мошенничества, 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)** - вид мошенничества - голосовой фишинг, использующий технологию, позволяющую автоматически собирать информацию, такую как номера карт и счетов.

Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

- автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции - перезвонить по определенному номеру немедленно. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, часто представляется вымышленным именем от лица финансовой организации;
- когда по этому номеру перезванивают, на другом конце провода отвечает типично компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона;
- как только номер введен, вишер становится обладателем всей необходимой информации (номер телефона, полное имя, адрес), чтобы, к примеру, обложить карту штрафом;
- затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как PIN-код, срок действия карты, дата рождения, номер банковского счета и т.п.

**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. 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.

**Вирус, поражающий банкоматы.** Вирус, отслеживает производимые операции и ворует информацию с пластиковых карт, передавая ее мошенникам.

**Шимминг** – разновидность Скимминга. Вместо накладки на щель приемника пластиковых карт банкоматов (скиммеров) используется очень тонкая, гибкая плата, внедряющаяся через эту щель внутрь банкомата. "Шим" подсаживается при помощи специальной карты-носителя: ее просовывают в щель банкомата, где тонкий "шим" подсоединяется к контактам, считывающим данные с карт, после чего карта-носитель удаляется. Дальше все работает, как и при традиционном скимминге — т.е. со вставляющихся в банкомат пластиковых карт считываются все важные данные, которые затем используются злоумышленниками для производства карт-дубликатов и снятия с их помощью денег.

**Заклеивание скотчем части банкомата**, которая выдает деньги (часть кэш-диспенсера). Снимаете деньги, а деньги не выходят. В состоянии чрезвычайной раздраженности забираете карту и уходите искать другой банкомат. Из-за угла выходит мошенник, внимательно наблюдавший за вами, отклеивает скотч и забирает деньги.