Центр правовой информации

Информационная памятка

Обоянь, 2023 г.

Скимминг вне закона

Скимминг – вид компьютерного мошенничества, при котором преступники с помощью спецоборудования для банкоматов копируют информацию с магнитной полосы банковской карты (в том числе пин-код) и выпускают ее клон.
Активное пользование картами провоцирует рост случаев мошенничества. В группе риска находятся люди, которые часто пользуются "пластиком" в том числе за границей и через сеть Интернет. Способы, которые применяют преступники, становятся все более сложными и технологичными, и сегодня попасть в поле действия мошенников можно, даже соблюдая все требования безопасности при использовании карты.
Чтобы не попасть в ловушку, нужно соблюдать несколько простых правил, быть внимательнее и осторожнее.

Большую часть платежей многие совершают при помощи карты. Но при необходимости снять или внести наличные можно через кассу банка (это время) или через круглосуточный банкомат.
Это удобно, но, к сожалению, не гарантирует безопасности при совершении операции через терминал.

С карты пропали деньги: кто виноват?

Неожиданная пропажа денег с карточного счета может объясняться разными причинами: происками мошенников, ошибочными действиями банка, торговой точки, платежной системы, а иногда даже самого владельца карты и т.п.
Мошенники хорошо маскируются. Во-первых, они выбирают банкоматы, находящиеся на улицах вне помещений. Во-вторых, снимают деньги, убедившись, что за ними никто не наблюдает. В-третьих, прикрывают лицо, человека в защитной маске и кепке, надвинутой на лоб, идентифицировать практически невозможно.
Кроме того, устройства для скимминга находятся внутри банкомата, и заметить их довольно сложно, особенно при недостаточном освещении.

Виды мошенничества с банковскими картами

- Воровство карт.

- Фальшивые терминальные устройства.
- Скимминг
- «Ливанская петля».
- Фишинг.
- Мошенничество на сайтах бесплатных объявлений.
- Мошенничество с картами в точках продажи товаров и услуг.
- Выигрыш призов.

Рынок пластиковых карт переживает новый этап развития. На первый план выходят ко-брендинговые и кобеджинговые проекты, предлагающие их обладателям возврат средств (cash-back) и премиальные баллы за полеты, бронь отелей и т. д. На Дальнем Востоке выпущено 8,2 млн пластиковых карт. Кредитные карты в этой доле занимают примерно 13%.

Банки не просто вернулись к их активному выпуску в последние годы, но в целом нарастили их эмиссию.

Активное пользование картами провоцирует рост случаев мошенничества.

Скимминг – это вид мошенничества, представляющий собой кражу данных карты при помощи специального устройства, вмонтированного в банкомат.

Skimming (от англ. skim – быстро читать) происходит так: данные карты считываются и передаются на сервер мошенникам, которые затем изготавливают дубликат пластика и снимают деньги.

Чтобы украсть содержимое карты, мошенникам нужно скопировать две вещи: магнитную полосу на карте и пин. Для этого у них в арсенале три устройства.

Скиммер. Это самодельный считыватель магнитной ленты. Мошенники прикрепляют его к картоприемнику банкомата. Иногда скиммер маскируют так хорошо, что распознать его не может даже сотрудник банка.

Скрытые камеры. Мошенники крепят их на банкомат или прячут где-то возле. Миниатюрная камера направлена на клавиатуру банкомата и записывает, как клиенты вводят пин. Отличить камеру непросто, ведь их ставит и служба безопасности банка.

Накладная клавиатура. Мошенники устанавливают на банкомат поддельную клавиатуру поверх оригинальной. Поддельная запоминает все, что вы набираете, и передает нажатия на настоящие клавиши. Банкомат реагирует на нажатия как

обычно, поэтому подмену заметить сложно. Потом преступники забирают накладку, расшифровывают запись и узнают пин.

Приёмы мошенничества

Фальшпанели и черные точки. Мошенники делают поддельные панели, монтируют в них видеокамеры, а потом незаметно крепят к банкомату: на диспенсер для денег, под козырек или под экран.

Внимательно изучите поверхность банкомата, потрогайте панели. Если что-то шатается, изучите деталь поближе.

Если на ровной поверхности встретилось миниатюрное углубление, которое издалека выглядит как черная точка, то, вероятно, это глазок видеокамеры.

Выпуклая или отличающаяся по тону клавиатура. У мошенников не всегда есть возможность покрасить фальшивые запчасти в цвет банкомата. Несовпадение по цвету и тону легко заметить.

Чаще всего фальш-клавиатуру крепят на клей или двусторонний скотч. Поэтому при наборе клавиш ощущается небольшой люфт, накладка отходит от банкомата.

Как выбрать банкомат

Банкоматы внутри отделений надежнее. Их лучше охраняют и чаще проверяют безопасники банков. К тому же в отделениях всегда много банкоматов: обклеить скиммерами каждый — слишком накладно для мошенников. В то же время преступники иногда специально атакуют именно отделения, ведь людям кажется, что там им ничего не угрожает.

«Крылья» для клавиатуры. Такие банкоматы затрудняют установку лжеклавиатур и почти полностью исключают возможность записи ввода пина на скрытую камеру.

Банкоматы с джиттерами. Джиттер — это накладка на картоприемник, которая заставляет карту вибрировать при вводе. Если банкомат снабжен джиттером, то, скорее всего, мошенники обойдут его стороной: дрожание не позволит им корректно скопировать магнитную ленту на карте. Без этого вся схема становится бессмысленной.

На страже закона

В связи с динамичным ростом числа преступлений, совершаемых в целях хищения денежных средств с использованием высоких технологий в банковской сфере, был

принят Федеральный закон от 08.06.2015 N 153, направленный на усиление уголовной ответственности за такие преступления. 5 декабря 2016 г. вступил в силу Указ Президента РФ N 646, утвердивший новую Доктрину информационной безопасности. Ранее Федеральным законом от 27.06.2011 N 161-ФЗ "О национальной платежной системе" было введено определение электронного средства платежа, под которым понимаются средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения для осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Что делать в скиммингговом банкомате

- Не забирайте фальш-детали, не открепляйте их и не привлекайте к себе внимание.
- Если дело происходит днем и внутри отделения, найдите сотрудника банка и спокойно расскажите ему о подозрениях.
- Если дело происходит на улице или ночью, уйдите подальше от банкомата, позвоните в банк, которому принадлежит банкомат, и опишите все, что Вы обнаружили.

Скимминг – это когда мошенники крадут данные карты через банкомат. Для этого они ставят на банкоматы специальные считыватели, скрытые камеры и накладные клавиатуры.

Осмотрите банкомат перед тем, как вставить карту. Ищите подозрительные признаки: накладки на картоприемник, фальшпанели, сколы и следы от клея.

Не стесняйтесь изучить поверхность банкомата. Если что-то держится плохо, лучше найти другой.

Пользуйтесь банкоматами внутри отделений банка.

Берегите пин. Прикрывайте руку свободной рукой, когда вводите его.