**Мошенники и банковские карты**

Мошенники и банковские карты

Появление банковских карт во многом облегчило жизнь людей. Теперь нам не нужно носить с собой крупные суммы денежных средств и бояться, что какой-нибудь воришка похитит кошелек. Практически все магазины принимают оплату пластиковыми картами, а если нет, то поблизости всегда есть банкомат. Но даже такой технический прогресс не гарантирует безопасность ваших сбережений. **На смену привычным для граждан «карманникам» пришли современные кибермошенники — скиммеры.**

**Скиммеры** - это мошенники, которые с помощью специальных устройств, считывающих информацию с банковских карт (скиммеров), путем определенных махинаций, снимают денежные средства со счетов граждан.

**Как же это происходит?**

Для того, чтобы узнать содержимое карты, мошенникам нужно скопировать две вещи: магнитную полосу на карте и ПИН-код. Для этого у них в арсенале три устройства.

**Скиммер** — миниатюрное считывающее переносное устройство, которое крепится к картридеру банкомата. Именно оно считывает всю информацию, записанную на магнитной полосе банковской карты. Получив данные, мошенники переносят их на заранее заготовленные фальшивые карты. Но без ПИН-кода они не могут реализовать свой преступный замысел, поэтому в ход идут другие снаряжения — скрытые камеры или накладные клавиатуры.

**Скрытые камеры** крепят на банкомат или прячут где-то рядом. Такая камера направлена на клавиатуру банкомата и записывает, как клиенты вводят ПИН-код. Также мошенники могут установить на банкомат **поддельную клавиатуру поверх оригинальной**. Она 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-код**.

Стоит отметить, что мошенники списывают средства со счетов граждан обычно ночью, чтобы потерпевший не успел заблокировать карту.

**Как же обезопасить свои средства от посягательств скиммеров?**

**-** Не стесняйтесь изучить поверхность банкомата. Потрогайте панели. Обычно фальшивые держатся плохо. Если что-то шатается, изучите деталь поближе.

**-** Плохой сигнал — если на ровной поверхности встретилось миниатюрное углубление, которое издалека выглядит как черная точка. Присмотритесь, возможно, это глазок видеокамеры.

**-** У мошенников не всегда есть возможность покрасить фальшивые запчасти в цвет банкомата. Несовпадение по цвету и тону легко заметить.

**-** Пользуйтесь только хорошо знакомыми банкоматами. Банкоматы в отделении банков находятся под наблюдением охранников и являются более безопасными. В людных местах и местах с большой проходимостью сложнее незаметно установить скиммеры. Банкоматы, находящиеся в глухих переулках и в плохо освещенных местах, больше всего подвержены риску, поэтому старайтесь ими не пользоваться.

**-** Прежде чем вставить вашу карту в банкомат, внимательно осмотрите картридер на присутствие в нем посторонних предметов, накладок, наклеек, вставок. По возможности пользуйтесь банкоматами, оснащенными антискиммерами — это такие пластиковые прозрачные насадки, которые наносятся на щель, куда вставляется карта.

**-** Считать информацию с карты также могут в кафе или магазине. Поэтому обязательно требуйте проведения операций с картой только в Вашем присутствии.

**-** Присмотритесь, если банкомат старый, со сколами и затертыми панелями, а клавиатура выглядит как новая, — это признак скиммеров. Не бывает, чтобы банки меняли клавиатуру отдельно от корпуса банкомата. Если клавиатура отличается по фактуре, выпирает или шатается, попробуйте поддеть ее ногтем.

**-** Если банкомат атакован мошенниками, под накладкой вы увидите настоящую клавиатуру. Чаще всего лже-клавиатуру приклеивают клеем или двусторонним скотчем. Поэтому при наборе клавиш ощущается небольшой люфт. Накладка как бы «отходит» от банкомата.

**-** Всегда прикрывайте ладонью панель клавиатуры. Это не позволит видео камере мошенников зафиксировать искомую комбинацию вашего ПИН-кода.

**-** Банкоматы, имеющие на клавиатуре специальные «крылья», затрудняют установку лже-клавиатур и почти полностью исключают возможность записи ввода ПИН-кода на скрытую камеру.

**-** Подключите услугу "СМС-банк", тогда Вы сможете быстро среагировать на внезапные списания.

**Что делать, если вам попался скимминговый банкомат?**

**1.** Не забирайте фальш-детали, не открепляйте их.

**2.** Заберите вещи и уходите подальше от банкомата. Не привлекайте к себе внимание, за вами могут следить из машины или пешком.

**3.** Убедитесь, что за Вами не следят. Потом позвоните в банк, которому принадлежит банкомат, и сообщите о случившемся.

**4.** Если вы заметили скиммер уже после того, как вставили карту, оставьте ее в банкомате. Позвоните в свой банк, заблокируйте и опишите ситуацию.







