****

**«Карта, я тебя знаю».**

**Что такое скимминг и как с ним бороться**

***Александр Вураско***

***Специалист по информационной безопасности***

На экране высвечивается сообщение: с карты списаны или сняты деньги. Вы хватаетесь за портмоне, предположив, что «пластик» потерян или украден — но нет, всё на месте. О том, кто тратит ваши деньги и как вору удалось до них добраться — читайте в материале.

Физически карта и правда похищена. Вернее, украдена её нематериальная суть: данные и пароли. Сценарии разные — мы уже рассказывали о [фишинге](https://sberclever.ru/sections/protection/376bd918-655a-4598-b96b-cb4566706308" \t "_blank) и [вишинге](https://sberclever.ru/sections/protection/1d9f35b3-c8de-4fb5-b1e6-e4ed36c25219" \t "_blank), когда жертва добровольно отдаёт сведения о карте (а они буквально на вес золота) в руки мошенников. Но сейчас речь пойдёт о другой технологии, не менее распространённой — о скимминге.

**Скимминг —** технология кражи данных банковской карты для последующего изготовления её копии. Классический скимминг подразумевает физическое взаимодействие устройства злоумышленников с картой жертвы. То есть вы должны вставить её в скомпрометированный банкомат или платёжный терминал.

В России скимминг практически изжит — ещё в 2019 году зампред правления Сбербанка Станислав Кузнецов заявил: «Фактически в нашей стране почти сведён данный вид мошенничества к нулю». Год спустя замдиректора департамента ЦБ РФ по информационной безопасности Артём Сычёв отмечал в беседе с журналистами, что в России «вообще

исчез» такой тип махинаций, как скимминг. «Есть факты, которые мы фиксируем, когда люди говорят, что с их карт что-то списали в банкомате — это 100% использование карты за рубежом. На территории Российской Федерации такое не работает», — сказал Сычёв.

Так и есть, однако не стоит забывать, что в мире распространены банкоматы и платёжные терминалы, которые считывают именно информацию с магнитной полосы — а значит, на них можно установить накладку и похитить данные карты. Скорее всего, когда мошенники попытаются снять деньги, ваш банк заблокирует подозрительную операцию, но шанс на успех у злоумышленников есть, хоть и небольшой. Не стоит его увеличивать своими руками — помните, что осторожность и осмотрительность никогда не вредят.

**Как мошенники это делают?**

Для воровства денег используется специальная накладка поверх картоприёмника (того самого отверстия в банкомате, куда мы, клиенты, вставляем карту). Она позволяет злоумышленникам считывать информацию с нашего «пластика». А для того, чтобы узнать пин-код, устанавливают или фальш-клавиатуру на банкомат, или миниатюрную камеру, направленную на панель ввода.

Главная задача считывателя — получить данные магнитной полосы карты и передать их на сервер мошенников. Считывание происходит в момент прохождения карты через накладку, наклеенную на картоприёмник банкомата.

Наверняка вы обращали внимание на то, что банкоматы разных моделей и разных банков имеют картоприёмники весьма причудливых форм. Это сделано не для красоты, а чтобы затруднить установку скимминговой накладки. Использование уникальных картоприёмников не позволяет создать универсальные считыватели и вынуждает злоумышленников изготавливать индивидуальные накладки для каждого банка и типа банкоматов, что требует дополнительных затрат.

Но считыватель не обязательно располагается на банкомате. Бывали случаи, когда он устанавливался на двери, ведущей в помещение с банкоматом. Под видом устройства, предназначенного для открывания двери в ночное время.

Со вторым компонентом — фальш-клавиатурой — всё просто: её накладывают поверх настоящей клавиатуры банкомата и фиксируют все

нажатия.

Из-за того, что многие современные банкоматы имеют нестандартные клавиатуры и специальные приспособления, затрудняющие установку фальш-панели, злоумышленники часто заменяют её на миниатюрную камер

у, расположенную либо на самом банкомате, либо в одном с ним помещении. Именно из-за возможности наличия скрытых камер следует прикрывать рукой клавиатуру банкомата, даже если рядом с вами никого нет.

Установка скимминговых накладок на банкомат занимает считанные секунды. Срок их жизни — как правило, пара часов, максимум день-два. Потом они снимаются, перезаряжаются и переносятся на новый банкомат. За это время накладки успевают обработать несколько сотен банковских карт, данные которых сохраняются в специальную базу.

Бывали случаи, когда банкомат заражался вредоносной программой, делавшей из него один большой скиммер. Но если вы имеете дело с банкоматами крупных банков, шансы встретить такое модифицированное устройство стремятся к нулю.

**Могут ли украсть карту другим способом?**

Да, через POS-терминал — устройство для обработки безналичных платежей. Встретить их можно в магазинах и киосках, кафе и ресторанах, гостиницах. Везде, где товар или услугу можно оплатить банковской картой. Они могут быть стационарными или портативными, но суть их работы не меняется. Такие терминалы взаимодействуют с вашей картой точно так же, как банкомат.

Иногда POS-терминал может быть перепрошит или заменён на модифицированный. В таком случае он приобретает дополнительный функционал, который может быть использован для создания копий прошедших через него банковских карт. При этом владелец заведения может не знать об этом, в отличие от его недобросовестных сотрудников.

Вы наверняка не раз сталкивались с ситуацией, когда, желая оплатить картой ужин в ресторане, давали её официанту. Он уходил с картой и вскоре возвращался с терминалом для оплаты. Делать так (вам, а не официанту) нельзя. Во-первых, отдавая карту в руки незнакомому человеку, вы даёте ему возможность записать её номер и реквизиты. Их будет достаточно для совершения некоторых типов онлайн-платежей (тех, где не требуется ввод кода из сообщения). Во-вторых, пока карта вне вашего поля зрения, сотрудник при помощи специального устройства может скопировать данные её магнитной полосы. А потом подсмотреть или заснять на миниатюрную видеокамеру вводимый вами пин-код.

Конечно, такой сотрудник сильно рискует. Если полиция проанализирует данные транзакций, то быстро обнаружит, что все карты жертв прошли через один терминал в одном заведении. Однако желающие испытать судьбу всё равно находятся.

**Что происходит с картами жертв скимминга**

Вариантов два: либо организаторы преступного бизнеса сами займутся изготовлением копий карт и хищением денег, либо продадут свою базу на чёрном рынке. Второй вариант более распространён. Сохранённые вместе с пин-кодами данные карты называются дампами. Они широко продаются в даркнете целыми массивами.

Приобретённые дампы записываются на банковские карты без опознавательных знаков (так называемый «белый пластик»). После чего вместе с пин-кодами передаются «дропам» — людям, специально нанятым для обналичивания денежных средств за процент от выведенной суммы. Они и будут ходить от банкомата к банкомату, раз за разом опустошая ваш счёт.

Сложность расследования скимминга заключается в том, что такие преступления совершаются участниками хорошо организованных преступных сообществ. В них существует чёткое разделение ролей, а участники зачастую даже не знакомы друг с другом и могут действовать на территории нескольких государств.

Момент компрометации карты совершенно незаметен для жертвы, а факты снятия цифровой копии карты и её неправомерного использования разнесены во времени вплоть до нескольких месяцев. Поэтому вы, скорее всего, никогда не узнаете, где и каким образом злоумышленники «считали» вашу карту. Исключения составляют случаи, когда полиции или службе безопасности банка удаётся обнаружить на банкомате скимминговую накладку или выяснить, каким банкоматом или POS-терминалом пользовались все потерпевшие.

**Что делать, если вы стали жертвой скиммеров**

1. Первое, что необходимо сделать, если с вашей карты без вашего ведома сняли деньги — обратиться в свой банк и сообщить о несанкционированной операции. Это позволит предотвратить дополнительные списания, а в ряде случаев и вернуть деньги.
2. Потом следует пойти в полицию и написать заявление. Только так есть шансы поймать мошенников.