Как защититься от скимминга

Что нужно знать, чтобы не стать жертвой мошенников

Бывает так: вы оказались в незнакомом месте без денег. Видите, в переулке банкомат. Снимаете наличные. Спустя несколько недель приходит СМС: некто в Кейптауне тоже снимает деньги с вашей карты.

Вы звоните в банк, блокируете карту, но деньги уже сняты. Вернут их или нет — зависит от банка. Придется разбираться и тратить время. Возможно, придется звонить в полицию Кейптауна.

Это называется скимминг: мошенники крадут данные карты, потом делают дубликат и обналичивают деньги. Опасность кроется прямо здесь:

Чтобы своровать содержимое карты, мошенникам нужно скопировать две вещи: магнитную полосу на карте и ПИН-код. 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-код. 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-код.

Как понять, что банкомат опасен

Перед тем, как вставить карту, осмотрите банкомат. Ищите подозрительные признаки.

Накладки на картоприемник. Если на банкомате установлен скиммер, то карта сначала проходит через специальный считыватель, а потом попадает в обычный картоприемник. Посмотрите, нет ли такой накладки на щели, в которую вставляется карта.

Если на банкомате стоит антискимминговая накладка (полупрозрачная штука из пластика), попробуйте качнуть или повернуть ее. Настоящая будет намертво прикреплена к банкомату. Поддельная люфтит, отходит и шатается.

Обычно мошенники монтируют шпионские устройства на несколько часов, потому что боятся проверок инспекторов. Поэтому они используют простые способы крепления — скотч, клей, честное слово.

Зачастую мошенники оставляют следы: щели, клеевые подтеки и сколы. Лучше не использовать банкомат, картоприемник которого выглядит так, будто кто-то ковырял его отверткой или облил клеем.

Фальшь-панели 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. Есть случаи, когда камеру прятали в стенде для рекламных брошюр того же банка.

АО КБ «Урал ФД».
Универсальная лицензия ЦБ РФ №249 от 09.04.2020 г.
Россия, 614066 г. Пермь, ул. Стахановская, д. 54 стр. Д. Тел. 8(342)240 10 40

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.

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 лже-клавиатуру приклеивают клеем или двусторонним скотчем. Поэтому при наборе клавиш ощущается небольшой люфт. Накладка как бы «отходит» от банкомата.

Если клавиатура отличается по фактуре, выпирает или шатается, попробуйте поддеть ее ногтем. Если банкомат атакован мошенниками, под накладкой вы увидите настоящую клавиатуру.

Если банкомат старый, со сколами и затертыми панелями, а клавиатура выглядит как новая, — это тоже плохой знак. Не бывает, чтобы банки меняли клавиатуру отдельно от корпуса банкомата.

Как выбрать банкомат

Со скиммерами можно никогда не столкнуться, если следовать нескольким правилам.

Нет: незнакомые банкоматы. Старайтесь снимать деньги в одном банкомате. Идеально, если вы запомните, как он выглядит (особенно клавиатуру и картоприемник).

Нет: уличные банкоматы. Там мошенникам проще установить считыватель или записать на камеру, как вы набираете ПИН-код.

Нет: банкоматы в темных местах. Даже если банкомат находится в помещении, недостаток света — это плохо. Можно не заметить подозрительных деталей. Если выбора нет, включите фонарик на телефоне и осмотрите банкомат.

Да: антискимминговые накладки. Банки воюют с карточными мошенниками. Например, ставят на банкоматы антискиммеры — специальные защитные накладки, которые мешают прикрепить считывающее устройство.

Ирония в том, что сначала антискиммеры были очень похожи на сами скиммеры. Люди запутались, поэтому сегодня антискиммеры делают из прозрачного пластика. Это помогает клиенту увидеть: внутри картоприемника нет сканеров, проводов и плат.

Впрочем, мошенники научились маскировать скиммеры под антискиммеры. Тут поможет тот же рецепт — не стесняться пошевелить картоприемник перед тем, как вводить карту.

Да: банкоматы внутри отделений. 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.

Да: «крылья» для клавиатуры. Такие банкоматы затрудняют установку лже-клавиатур и почти полностью исключают возможность записи ввода ПИН-кода на скрытую камеру.

Да: 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.

Правда, с джиттерами есть проблемы. Во-первых, на большинстве банкоматов их нет. Во-вторых, понять, что на банкомате стоит джиттер, нельзя, пока вы не вставите карту. Но можно сначала протестировать незнакомый банкомат с помощью какой-нибудь дисконтной карты. Если она вибрирует при вводе, значит, банкомат безопасный.

Протестировать банкомат — это лишнее действие, но оно может сохранить вам и тысячу рублей, и пять, и пятьдесят. Помните: чтобы данные карты попали к мошенникам, достаточно один раз воспользоваться зараженным банкоматом.

Осторожно: банкомат в офисе или торговом центре. Скиммерам сложнее к ним подобраться. Но есть случаи, когда мошенники подкупали охрану, а те направляли камеры внутреннего наблюдения на банкомат. Потом видеозаписи передавались мошенникам, и они подсматривали ПИН-коды. Всегда прикрывайте клавиатуру рукой.

Осторожно: замки при входе в отделение банка. У многих банков есть отделения с магнитным замком. Войти туда можно с помощью любой карты с магнитной полосой. Иногда мошенники ставят скиммеры прямо на замок. Бороться с этим просто: заходите по дисконтной карте.

Иногда мошенники вешают на внешний замок клавиатуру для ввода ПИН-кода. Тут тоже просто: если на входе от вас требуют что-то вводить, это точно мошенники — причем отчаянные. Банки никогда не попросят вас ввести ПИН-код при входе в отделение.

Осторожно: туристические районы за границей. Когда мы путешествуем, мы не знаем, как выглядят банкоматы зарубежных банков, поэтому обмануть нас проще. Мошенники этим пользуются. Будьте внимательнее, особенно в Азии: азиатское скимминговое кунг-фу не знает равных.

Как защитить деньги

Прикрывайте руку свободной рукой, когда вводите ПИН. Иногда преступники не ставят камеры и накладные клавиатуры, а просто нанимают людей, которые подсматривают, как вы набираете ПИН-код.

Перейдите на чипованную карту. Наличие чипа не обезопасит вас на 100%. Чип действительно сложно скопировать. Но его считывает банкомат, а в России далеко не все банкоматы это умеют. Мошенники знают, где найти банкоматы устаревшего образца и снимают наличность по магнитной полосе. Чипы понижают риск, но не сводят его к нулю.

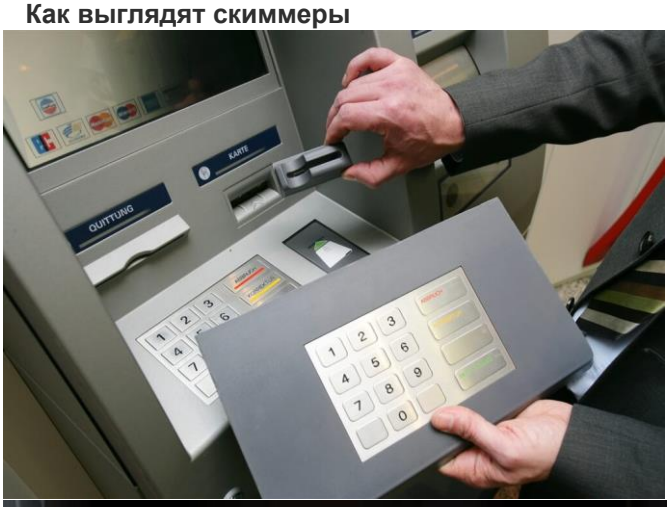
Подключите СМС-банк. Подключите СМС обо всех операциях по счету, чтобы быстро реагировать на внезапные списания. Это не поможет, если обналичивать будут ночью или если у вас выключен телефон.

Поставьте лимиты. Ограничьте в интернет-банке выдачу наличных. Мошенники не смогут снять всю сумму за один раз.

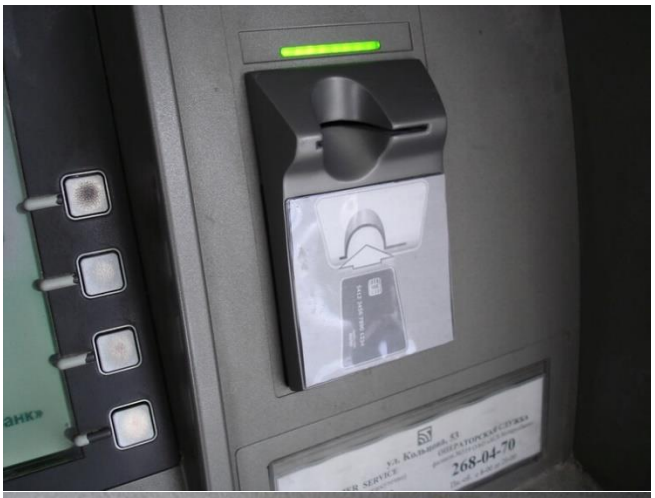
Что делать, если вам попался скимминговый банкомат

1. Не забирайте фальшь-детали, не откреплляйте их и не привлекайте к себе внимание.
2. Если дело происходит днем и внутри отделения, найдите сотрудника банка и спокойно расскажите ему о подозрениях.
3. Если дело происходит на улице или ночью, заберите вещи и уходите подальше от банкомата. За вами могут следить из машины или пешком — уйдите от преследования.
4. Убедитесь, что хвоста нет. Потом позвоните в банк, которому принадлежит банкомат, и в красках опишите все, что с вами случилось.
5. Если вы заметили скиммер уже после того, как вставили карту, оставьте ее в банкомате. Позвоните в свой банк и заблокируйте ее, но уже потом, когда окажетесь в безопасном месте.

Как выглядят скиммеры



АО КБ «Урал ФД». Универсальная лицензия ЦБ РФ №249 от 09.04.2020 г.
Россия, 614066 г. Пермь, ул. Стахановская, д. 54 стр. Д. Тел. 8(342)240 10 40




CASH


CARD


CHASE
DEBIT CARD


DIEBOLD


Bank of America