Защита банковских карт

Способы мошенничества

Мошенники часто имитируют **неисправность банкоматов**. Например, поздно вечером вы возвращаетесь домой и решаете по пути обналичить зарплату. Вставили карту, ввели PIN-код, сумму — всё идёт прекрасно. Картоприёмник отдал карту, но лоток, где должны появиться деньги, не открывается. Сломался? Наверное! Вокруг темно, нужно позвонить в банк и разобраться, что случилось. Вы отошли буквально на десять метров, а шустрые воришки уже отклеили скотч и забрали ваши деньги. Да-да, купюры не выпускала простая клейкая лента.

- Впрочем, банкомат может быть настоящим и даже исправным. Это не проблема, если у злоумышленников есть **скиммер**. Это устройство для считывания информации, закодированной на магнитной полосе карты. Физически скиммер представляет собой накладной блок, прикрепляемый к картоприёмнику, при этом он выглядит как часть конструкции банкомата.

При помощи передатчика мошенники получают информацию со скиммера и изготавливают поддельные карты. Они будут пользоваться скиммированной картой, но деньги будут списываться со счёта оригинальной. Отсюда название метода — скимминг, от английского «снимать сливки».
Как они узнают PIN-код? В дополнение к скиммеру у них есть другие девайсы. Например, **накладная клавиатура**. Она полностью имитирует настоящую, но при этом запоминает набираемые комбинации клавиш.

- **Фишинг** — распространённый способ интернет-мошенничества. Большинству из вас не нужно объяснять, что это такое. Возможно, кто-то даже получал «письмо от банка» с просьбой перейти по ссылке и уточнить реквизиты. Причём фишинговая страница выглядела как настоящая, те же цвета, шрифты, логотипы, за исключением досадной «опечатки» в адресной строке.
- В последнее время всё больше распространяется подвид фишинга — **вишинг**. Проще говоря, **развод по телефону**. Мошенники моделируют звонок автоинформатора. Пугающий роботизированный голос сообщает вам, что ваша карта заблокирована, или подверглась атаке хакеров, или вам срочно нужно погасить долг по кредиту. За подробностями звоните по такому-то номеру. Вы звоните, и учтивый «оператор» просит вас «сверить» номер карты, срок её действия, верификационный код… Как только вы продиктовали последнюю цифру, можете попрощаться со своими деньгами. Пока вы придёте в себя, их уже потратят в каком-нибудь интернет-магазине.

Правила безопасности при использовании карт

- Оформив в банке дебетовую или кредитную карту, мы получаем договор банковского обслуживания и конверт с PIN-кодом. Жаль, что в дополнение к этому набору не прикладывают памятку с элементарными правилами безопасности для держателей карт. В неё следовало бы включить следующие рекомендации.
- По возможности сделайте себе гибридную карту — с чипом и магнитной полосой (к сожалению, карты только с чипом в России почти не используются). Такая карта лучше защищена от взлома и подделки путём скимминга.
- Выучите PIN-код наизусть. Если же на память надежды нет, запишите его на листочек, но храните отдельно от карты.
- Никогда, ни при каких обстоятельствах не сообщайте третьим лицам PIN-код и CVV2-код карты, а также срок её действия и на кого она зарегистрирована. Ни один банк не будет спрашивать у вас эти реквизиты. А для зачисления средств на ваш счёт достаточно лишь 16-значного номера, указанного на лицевой стороне карты.
- Не используйте так называемые зарплатные карты для расчётов в магазинах и оплаты интернет-покупок. Деньги с карточного счёта лучше переводить на лицевой либо устанавливать суточные лимиты на все виды совершаемых операций.
- Выбирайте банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения.
- Не пользуйтесь подозрительными моделями банкоматов. А прежде чем вставить карту в терминал, внимательно осмотрите его. Нет ли чего-нибудь подозрительного на клавиатуре или в картоприёмнике? Не висит ли поблизости странный лоток с рекламой?
- Не стесняйтесь закрывать клавиатуру рукой и просить отойти в сторону особо любопытных товарищей в очереди. При возникновении проблем не пользуйтесь советами «случайных помощников» — никуда не уходя, сразу звоните в банк и блокируйте карту.
- Если вы потеряли карту, а также если у вас есть основания полагать, что третьи лица узнали её реквизиты, немедленно обратитесь в банк и заблокируйте её.

Правила безопасности при пользовании банкингом

Банкинг — дистанционное банковское обслуживание.

- Не входите в интернет-банк с чужих компьютеров или из публичных незащищённых сетей. Если же это всё-таки случилось, по завершении сессии нажмите «Выход» и очистите кеш.
- На личном компьютере установите антивирус и своевременно его обновляйте. Используйте современные версии браузера и почтовых программ.
- Не скачивайте файлы, полученные из непроверенных источников, не переходите по ненадёжным ссылкам. Не открывайте подозрительные письма и сразу же блокируйте их отправителя.
- Без необходимости не вводите никакие свои персональные данные, помимо логина и пароля.
- Проверяйте адресную строку. Должно использоваться защищённое HTTPS-соединение. А малейшее несовпадение с доменом банка почти наверняка означает, что вы находитесь на фишинговом сайте.
- Придумайте сложный пароль для входа в личный кабинет, а также используйте одноразовые пароли, запрашиваемые банками для подтверждения действий в личном кабинете.

Выводы:

- Итак, краткий алгоритм действий при незаконном списании средств с банковской карты таков:
- Не паникуем, звоним в банк и блокируем карту. Плюс просим оператора назвать остаток на счету и последние совершённые транзакции.
- В течение суток бежим в банк и пишем заявление. Обязательно визируем у уполномоченного сотрудника банка свой экземпляр заявления.
- Если сотрудники кредитного учреждения каким-либо образом препятствуют этому и отказываются принять заявление (закончились бланки, технический перерыв и так далее), обращаемся в прокуратуру.
- Пишем заявление в полицию. Особенно если вы столкнулись с грабежом или разбоем.
- Ждём возврата денег.
- Если банк отказывается возмещать средства, списанные с карты, ссылаясь, например, на нарушение порядка использования электронных денежных средств, вы можете отстаивать свои права в суде.