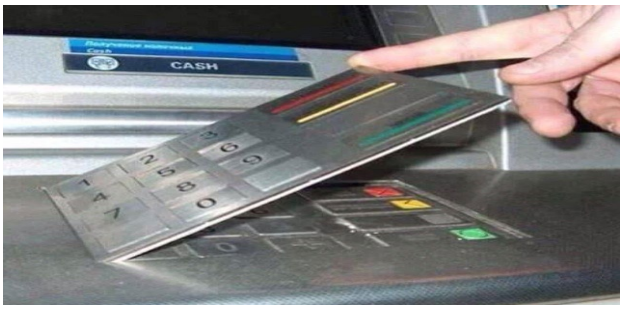
Что такое скимминг карточек и как себя защитить

Что такое скимминг карточек?

Скиммер карточек - это незаконное устройство, которое преступники прикрепляют к устройствам для считывания карточек в банкоматах (Automated Teller Machines - ATM), на терминалах в точках продаж (Point-of-Sale - POS) или на бензоколонках. Преступники могут использовать данные, считанные с магнитной полосы, чтобы украсть личные данные потерпевшего или изготовить поддельные дебетовые, кредитные или карточки электронного перевода пособий (Electronic Benefits Transfer - EBT), которые могут быть использованы для оплаты покупок и кражи денег или пособий потерпевшего. Скиммеры карточек трудно обнаружить, поскольку они сконструированы таким образом, чтобы сливаться с терминалом.

Как определить устройства для скимминга карточек, камеры с отверстиями и поддельные клавиатуры:

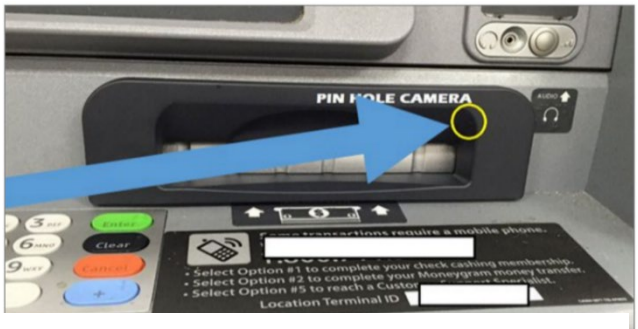
- Большинство устройств для скимминга используются в банкоматах и POS-терминалах и устанавливаются сверху на настоящее реальное устройство для считывания карточек; однако на автозаправочных станциях они также могут быть спрятаны внутри за устройством для считывания карточек.
- Поддельные накладки на клавиатурах также могут быть использованы для записи PIN-кода.



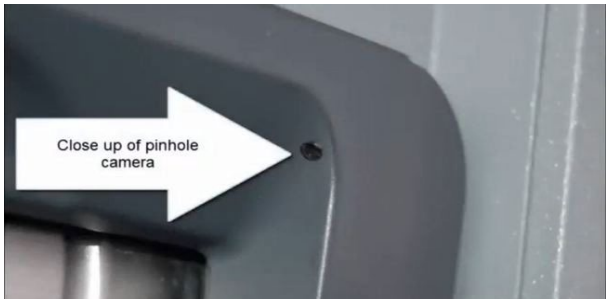
From: Engadget
https://www.engadget.com/2014-07-28-credit-card-skimming-explainer.html

om: FMB
ps://ibankfmb.com/2018/06/how -to-spot-and-avoid-card-skimmers/

- Камеры с отверстиями могут быть размещены над или вокруг PIN панели или установлены на банкомате для записи действий клиента в момент ввода им PIN-кода.



From: Cambridge PD
https://www.universalhub.com/2016/debit-card-reading-skimmer-found-cambridge-atm

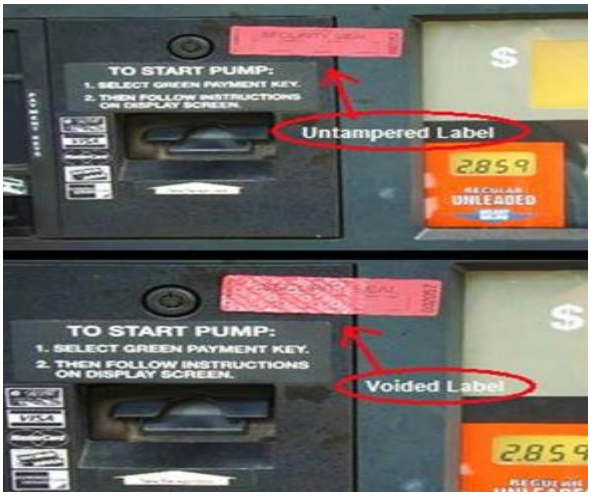


From: *East Lampeter Township Police Department YouTube Video*
https://local21news.com/news/local/photos -how -to -detect -skimming -devices -on -atms

RUSSIAN

Советы по использованию карточек на автозаправочных станциях:

- Обратите внимание на защитную ленту, наклеенную на панель корпуса автозаправочного насоса. Если панель была вскрыта, на защитной ленте будет написано "void" ("недействительно").
- Ищите устройства для скимминга, установленные сверху устройств для считывания карточек на автозаправочных станциях.
- По возможности, воспользуйтесь кредитной карточкой вместо дебетовой, чтобы не вводить свой PIN-код. Кредитные карточки также могут обеспечить дополнительную защиту от мошенничества.
- Используйте бензоколонки, расположенные ближе к обслуживающему персоналу, или производите оплату внутри автозаправочной станции.



From National Association of Convenience Stores (NACS) and Conexxus
https://www.ftc.gov/business-guidance/blog/2017/06/best-practices-foil-gas-station-skimmers

Как избежать скимминга карточек:

- Визуально и физически осматривайте банкоматы и POS-машины, прежде чем провести или вставить свою карточку. Не болтается ли она или не кажется ли незакрепленной? Если это так, не проводите и не вставляйте свою карточку, сообщите об этом работникам бизнеса и местным правоохранительным органам.
- Прикрывайте клавиатуру, когда вводите PIN-код, и никогда никому не сообщайте свой PIN-код.
- Используйте карточку с встроенным чипом, если она у вас есть.
- Используйте бесконтактные карточки или телефоны для безопасных и простых платежей, прикладывая карточку или телефон к терминалу для бесконтактных платежей.
- Подпишитесь на уведомления или оповещения о транзакциях по банковским и кредитным карточкам, и вы будете получать уведомления или оповещения при каждом использовании вашей карточки.
- Расплачивайтесь наличными везде, где это возможно.
- POS/ATM-терминалы в туристических зонах являются популярными объектами для использования скимминговых устройств. Будьте особенно осторожны в таких местах.

Советы для пользователей карточек EBT, чтобы избежать скимминга:

- Округ или штат никогда не будут звонить или отправлять текстовые сообщения с целью узнать номер вашей карточки EBT или PIN-код.
- Проверьте свой баланс карточки EBT и убедитесь, что не было произведено несанкционированных платежей на вебсайте: EBT.CA.GOV.
- Избегайте использования несанкционированных приложений от независимых производителей для проверки баланса вашей карточки EBT. Если вы заметили несанкционированные платежи, сообщите о них в Управление социального обеспечения населения (DPSS) по телефону (866) 613-3777 или в местное отделение DPSS.
- Если вы подозреваете, что ваш PIN-код был взломан, вы можете изменить его в любое время, позвонив по телефону горячей линии Службы поддержки клиентов системы EBT в штате Калифорния (California EBT Customer Service Helpline) по телефону (877) 328-9677 или в местном отделении DPSS.
- Если у вас есть банковский счёт, вы, возможно, сможете перечислять свои денежные пособия непосредственно на свой банковский счёт.

Что нужно делать, если кредитная или дебетовая карточка подверглась скимингу:

- Если ваша кредитная или дебетовая карточка подверглась скимингу, обратитесь в местные правоохранительные органы, чтобы подать заявление.
- Немедленно сообщите о подозрительных действиях или несанкционированных платежах компании, выдавшей вашу карточку. Как правило, у вас есть 60 дней с даты получения счета, чтобы подать иск на оспаривание. Посетите вебсайт: dcba.lacounty.gov/portfolio/credit-card-disputes для получения дополнительной информации о том, как оспорить несанкционированные платежи.
- Вы также можете бесплатно установить оповещения о мошенничестве или замораживание кредитов, обратившись в три основных агентства по кредитным историям. Посетите вебсайт: dcba.lacounty.gov/your-credit для получения дополнительной информации об оповещениях о мошенничестве и замораживании кредитов.
- Дополнительную информацию можно найти по ссылке «10 способов распознать, стали ли вы жертвой кражи личных данных, и какие действия вы можете предпринять» (10 Ways to Recognize If You Are A Victim of Identity Theft and Actions You Can Take).
- Если вы стали жертвой кражи личных данных, воспользуйтесь руководством DCBA «Справочник по краже личных данных» (Identity Theft Toolkit), которое поможет привести вашу кредитную историю в порядок.

Что делать, если ваша карточка EBT подверглась скимингу:

- Сообщайте о любых несанкционированных платежах в DPSS по телефону (866) 613-3777 или посетите местное отделение DPSS.
- Вы должны сообщить об украденных пособиях CalFresh в течение десяти дней с даты электронного хищения, чтобы иметь право на замену украденных пособий.
- Вы должны заполнить электронную форму о краже денежной помощи (Electronic Theft of Cash Aid Form - EBT 2259) в течение 90 дней с момента электронной кражи, чтобы получить замену продовольственных или денежных пособий.
- Сообщайте о мошенничестве в сфере социального обеспечения на горячую линию Департамента социальных услуг штата Калифорния (CDSS) по телефону (800) 344-8477, или на Центральную линию DPSS для сообщений о мошенничестве по телефону (800) 349-9970, или на вебсайте dpss.lacounty.gov/en/web-forms/report-fraud.html

- Сообщите о потерянной или украденной карточке EBT в Отдел по обслуживанию клиентов CDSS по телефону (877) 328-9677, в Центр по обслуживанию клиентов DPSS по телефону (866) 613-3777 или посетите местное отделение DPSS.
- Вы также можете бесплатно установить оповещения о мошенничестве или замораживание кредитов, обратившись в три основных агентства кредитных историй. Посетите вебсайт dcba.lacounty.gov/your-credit для получения дополнительной информации об оповещениях о мошенничестве и замораживании кредитов.
- Дополнительную информацию можно найти на вебсайте «10 способов распознать, являетесь ли вы жертвой кражи личных данных, и какие действия вы можете предпринять» (10 Ways to Recognize If You Are A Victim of Identity Theft and Actions You Can Take).
- Если вы стали жертвой кражи личных данных, воспользуйтесь руководством DCBA «Справочник по краже личных данных» (Identity Theft Toolkit), которое поможет привести вашу кредитную историю в порядок.