

آشنایی با دستگاه دزدی اطلاعات کارت‌ها و چگونگی محافظت از خود در برابر آن

دزدی اطلاعات کارت (اسکیم شدن کارت) چیست؟

دستگاه دزدی اطلاعات کارت (اسکیم کردن) یک دستگاه غیرقانونی است که مجرمین روی کارت‌خوان‌های ماشین پرداخت خودکار (ATM)، پایانه‌های نقطه فروش (POS) و یا پمپ‌های بنزین نصب می‌کنند. مجرمین از داده‌های به‌دست‌آمده از روی نوار مغناطیسی استفاده می‌کنند تا هویت قربانی را به سرقت ببرند یا کارت‌های جعلی اعتباری، بانکی یا کارت الکترونیک انتقال مزایا (EBT) بسازند که برای خرید و سرقت پول یا مزایای فرد قربانی مورد استفاده قرار گیرد. دستگاه‌های دزدی اطلاعات کارت به‌سختی قابل شناسایی هستند، زیرا برای ترکیب شدن با پایانه، طراحی شده‌اند.

شناسایی دستگاه‌های دزدی اطلاعات کارت، دوربین روزنه‌ای ریز، صفحه‌کلید جعلی:

- اکثر دستگاه‌های دزدی اطلاعات کارت مورد استفاده در پایانه‌های ATM و POS، بر روی دستگاه کارت‌خوان اصلی قرار می‌گیرند، با وجود این در ایستگاه‌های پمپ بنزین این دستگاه‌ها می‌توانند در قسمت داخلی زیر کارت‌خوان نیز پنهان شوند.
- جلد کارت‌خوان‌های جعلی می‌تواند برای ضبط PIN (پین) نیز مورد استفاده قرار گیرد.



From: Engadget

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



From: FMB

<https://ibankfmb.com/2018/06/how-to-spot-and-avoid-card-skimmers/>

- دوربین‌های روزنه‌ای ریز در قسمت بالایی و یا دور صفحه کلید قرار می‌گیرند یا بر روی ATM نصب می‌شوند تا هنگام ورود رمز مشتری به دستگاه، آن را ضبط کنند.



From: Cambridge PD

<https://www.universalhub.com/2016/debit-card-reading-skimmer-found-cambridge-atm>

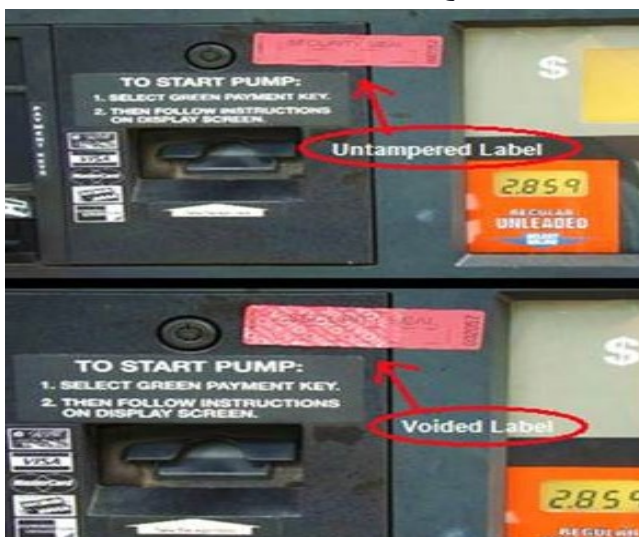


From: East Lampeter Township Police Department YouTube Video

<https://local21news.com/news/local/photos-how-to-detect-skimming-devices-on-atms>

نکاتی جهت استفاده کارت در ایستگاه‌های پمپ بنزین:

- به دنبال نوار امنیتی نصب شده بر روی پنل کابینت پمپ بنزین بگردید. چنانچه پنل دستکاری شده باشد، روی نوار امنیتی کلمه «VOID» را خواهید دید.
- به دنبال دستگاه‌های دزدی اطلاعات کارت که در بالای کارتخوان‌های ایستگاه پمپ بنزین نصب شده‌اند، بگردید.
- در صورت امکان، برای جلوگیری از وارد کردن پین خودتان، به جای کارت بانکی از کارت اعتباری استفاده کنید. کارت‌های اعتباری همچنین ممکن است محافظت بیشتری در برابر تقلب داشته باشند.
- از پمپ بنزین واقع شده به نزدیکترین متصدی استفاده کنید یا مبلغ را در داخل ایستگاه پمپ بنزین پرداخت کنید.



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

چگونه می‌توان از دزدیده شدن اطلاعات کارت جلوگیری کرد:

- قبل از اینکه کارت خود را بکشید یا آن را وارد کنید، دستگاه‌های ATM و POS را به صورت بصری و فیزیکی واریسی کنید. آیا دستگاه شل است یا تکان می‌خورد؟ در این صورت کارت خود را نکشید یا وارد دستگاه نکنید، به متصدی و مأموران محلی اجرای قانون اطلاع دهید.
- هنگام وارد کردن رمز خودتان، صفحه کلید را بیوشانید و هرگز رمز خود را به کسی ندهید.
- در صورت داشتن کارت دارای تراشه، از آن استفاده کنید.
- برای پرداخت امن و آسان، با قراردادن کارت یا تلفن روی پایانه‌های پرداخت بدون تماس، از کارت‌ها و یا تلفن‌های بدون تماس استفاده کنید.
- برای دریافت اعلان‌ها یا هشدارها در مورد معاملات بانکی و کارت اعتباریتان، ثبت نام کنید تا پس از هر بار استفاده از کارتتان، اعلان یا هشدار دریافت کنید.
- در صورت امکان، به صورت نقدی پرداخت کنید.
- پایانه‌های POS/ATM موجود در مناطق توریستی، اهداف مطلوبی برای دستگاه‌های دزدی اطلاعات کارت هستند. در این مناطق بیشتر مراقب باشید.

نکاتی برای استفاده‌کنندگان کارت EBT جهت جلوگیری از دزدیده شدن اطلاعات کارتشان:

- شهرستان لس‌آنجلس یا ایالت کالیفرنیا هرگز شماره کارت EBT تان و یا رمز آن را از طریق تلفن یا پیامک درخواست نخواهند کرد.
- موجودی کارت EBT تان و هزینه‌های غیرمجاز را در EBT.CA.GOV بررسی کنید.
- از استفاده از اپلیکیشن‌های غیرمجاز و طرف ثالث جهت بررسی موجودی کارت EBT تان خودداری کنید. در صورت مشاهده هرگونه هزینه غیرمجاز، مراتب را به دپارتمان خدمات فراگیر اجتماعی (DPSS) به شماره 613-3777 (866) یا به دفتر منطقه‌ای DPSS که در آن پرونده دارید، گزارش کنید.
- اگر مشکوک هستید که رمزتان در معرض خطر است می‌توانید هر لحظه با خط کمک خدمات مشتریان کارت EBT کالیفرنیا به شماره 328-9677 (877) یا با دفتر منطقه‌ای DPSS تماس بگیرید و آن را عوض کنید.
- اگر حساب بانکی دارید، ممکن است قادر باشید مزایای نقدی خود را مستقیماً به حساب بانکی‌تان واریز نمایید.

اگر اطلاعات کارت اعتباری یا بانکی‌تان دزدیده شود، چه باید بکنید:

- اگر اطلاعات کارت اعتباری یا بانکی‌تان دزدیده شود با مأموران محلی اجرای قانون برای ارسال گزارش تماس بگیرید.
- هرگونه فعالیت مشکوک یا هزینه‌های غیرمجاز را سریعاً به صادرکننده کارتتان گزارش کنید. معمولاً 60 روز از تاریخ صورت‌حساب بانکی‌تان فرصت دارید تا این اختلاف را گزارش کنید. جهت اطلاعات بیشتر در مورد چگونگی اعتراض به هزینه‌های غیرمجاز از dcba.lacounty.gov/portfolio/credit-card-disputes بازدید کنید.
- همچنین می‌توانید در تماس با سه شرکت اصلی گزارش‌دهی اعتباری هشدارهای رایگان تقلب یا مسدود کردن اعتبار تنظیم کنید. برای اطلاعات بیشتر در مورد هشدارهای تقلب و مسدود کردن اعتبار از dcba.lacounty.gov/your-credit بازدید کنید.
- اطلاعات بیشتر را می‌توانید در «10 راه برای تشخیص اینکه آیا قربانی سرقت هویت شده‌اید و اقداماتی که می‌توانید انجام دهید» مشاهده کنید.
- چنانچه قربانی سرقت هویت شده‌اید، از Identity Theft Toolkit مربوط به DCBA، برای برگرداندن اعتبارتان استفاده کنید.

اگر اطلاعات کارت EBT تان دزدیده شود، چه باید بکنید:

- هرگونه هزینه غیرمجاز را به DPSS به شماره 613-3777 (866) گزارش کنید یا از دفتر منطقه‌ای DPSS بازدید کنید.
- سرقت مزایای CalFresh را باید طی ده روز از تاریخ تراکنش سرقت الکترونیک گزارش کنید تا واجد شرایط جایگزینی مزایای سرقت شده باشید.
- جهت جایگزینی مزایای نقدی و مواد غذایی، باید فرم سرقت الکترونیک کمک نقدی (EBT 2259) را طی 90 روز از تاریخ تراکنش سرقت الکترونیک، کامل کنید.
- تقلب در برنامه رفاه را به خط ویژه تقلب در برنامه رفاه دپارتمان خدمات اجتماعی کالیفرنیا (CDSS) به شماره 344-8477 (800) یا به خط مرکزی گزارش تقلب DPSS به شماره 349-9970 (800)، یا به dpss.lacounty.gov/en/web-forms/report-fraud.html گزارش کنید.
- سرقت یا مفقود شدن کارت EBT تان را به بخش خدمات مشتریان CDSS به شماره 328-9677 (877)، مرکز خدمات مشتریان DPSS به شماره 613-3777 (866) گزارش کنید یا به دفتر منطقه‌ای DPSS بروید.

- همچنین می‌توانید با تماس با سه آژانس گزارش اعتبار، یک هشدار رایگان تقلب یا مسدود کردن اعتبار تنظیم کنید. برای اطلاعات بیشتر در مورد هشدار تقلب و مسدود کردن اعتبار از dcbalacounty.gov/your-credit بازدید کنید.
- اطلاعات بیشتر را می‌توانید در «10 راه برای تشخیص اینکه آیا قربانی سرقت هویت شده‌اید و اقداماتی که می‌توانید انجام دهید» مشاهده کنید.
- چنانچه قربانی سرقت هویت شده‌اید، از [Identity Theft Toolkit](#) مربوط به DCBA، برای برگرداندن اعتبارتان استفاده کنید.