

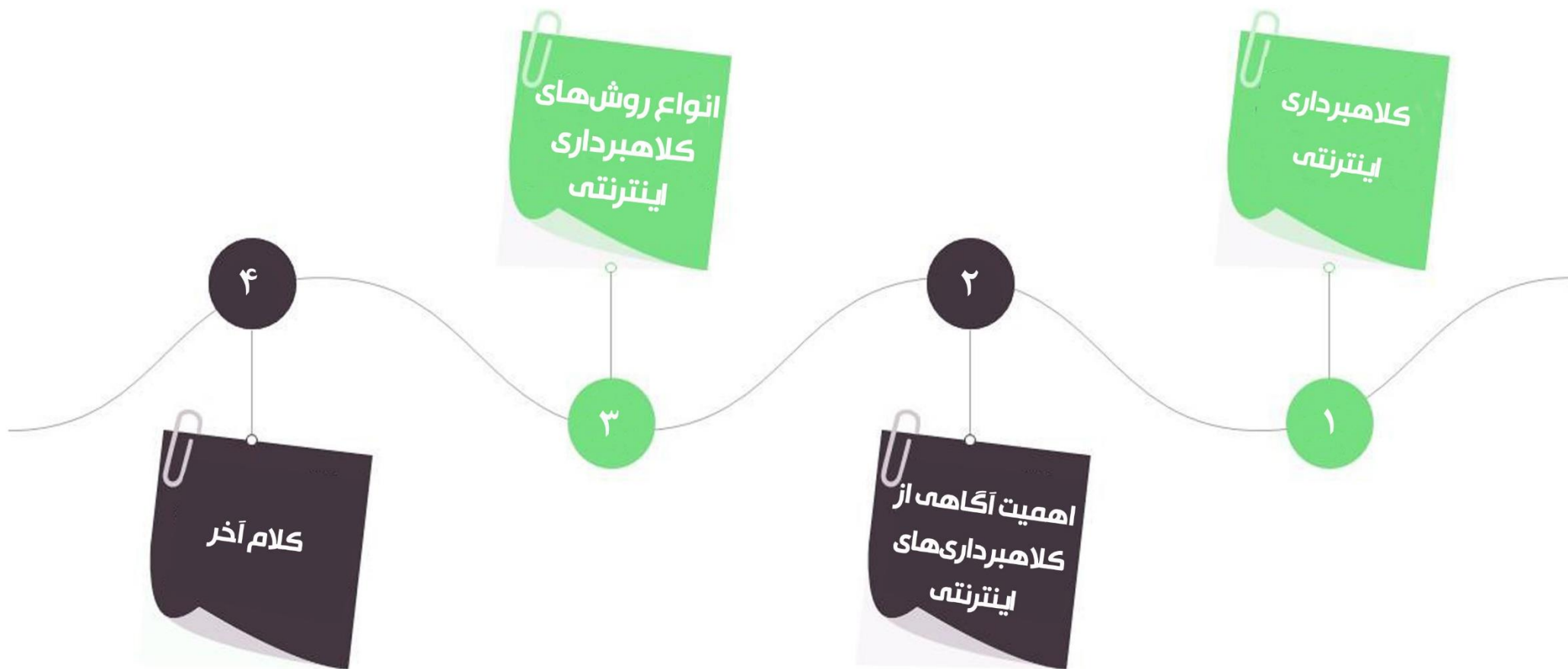
بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



انواع کلاهبرداری اینترنتی و روش‌های مقابله با آنها

کاری از مرکز نسرا استان‌های لرستان و اردبیل

دریك نگاه



کلاهبرداری اینترنتی چیست؟

هر عمل خلاف قانونی که توسط **رایانه یا سایر ابزارهایی که به اینترنت متصل می‌شوند**، انجام شود به نحوی که به صورت **مادی یا معنوی** آسیبی را با مردم برساند، مصداق بارز جرم در فضای آنلاین است.



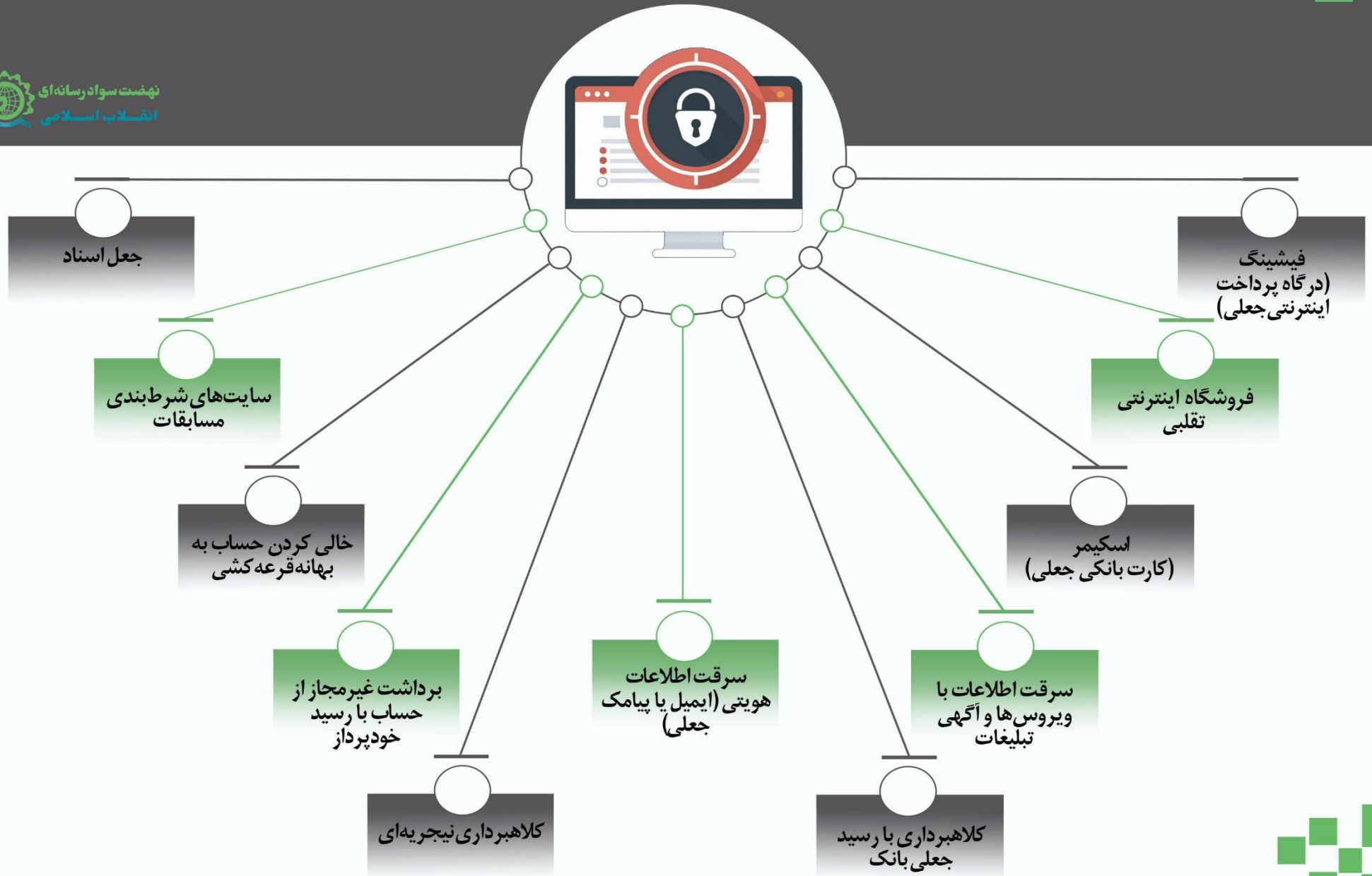
اهمیت آگاهی از کلاهبرداری‌های اینترنتی



با توجه به اینکه بسیاری از فعالیت‌های روزمره افراد به صورت **آنلاین** انجام می‌شود، افزایش آگاهی در مورد کلاهبرداری‌های اینترنتی می‌تواند به کاربران کمک کند تا از **خطرات احتمالی** جلوگیری کرده و اطلاعات شخصی و مالی خود را در امان نگه‌دارند.

انواع روش های کلاهبرداری اینترنتی

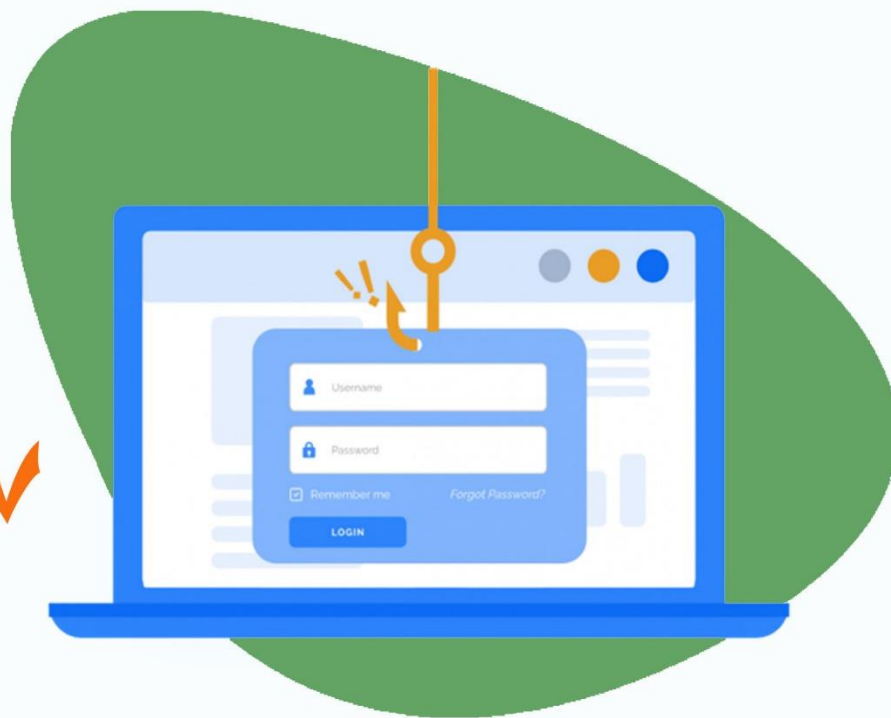
۳



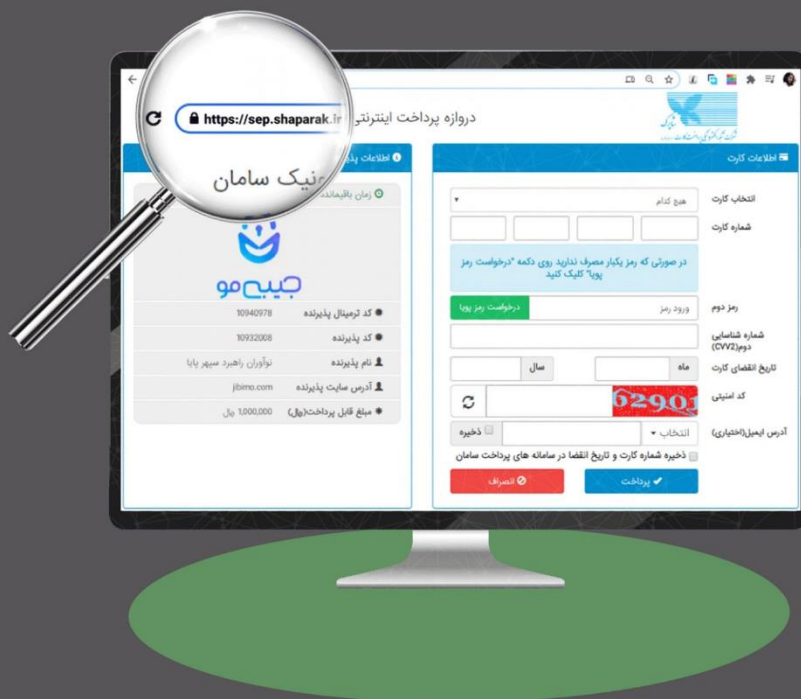
در این روش کلاهبرداران **صفحه درگاهی کاملاً مشابه** درگاه پرداخت‌های واقعی می‌سازند و اطلاعات حساب یعنی شماره کارت، رمز دوم و...، را ذخیره می‌کنند و در فرصت مناسب حساب بانکی افراد را خالی می‌کنند.

کلاهبرداران در این روش برای جلوگیری از ایجاد شک در ذهن کاربران پس از دریافت تمامی اطلاعات کارت از جمله رمز کارت **پیغام خطا در اتصال به بانک یا عدم انجام تراکنش** را نشان می‌دهند.

✓ حدود **۵۰ درصد** کلاهبرداری‌های اینترنتی را تشکیل می‌دهد.



نحوه تشخیص و مقابله با درگاه پرداخت جعلی



- * بررسی ارتباط ایمن
- * چک کردن آدرس صفحه پرداخت
- * وارد کردن اطلاعات نادرست
- * نصب افزونه ضد فیشینگ
- * راه اندازی مجدد
- * حذف رمز دوم و استفاده از رمز پویا

فیشینگ (درگاه پرداخت اینترنتی جعلی)

آدرس وبسایت و مطابقت
 املائی آدرس با جدول بالا

علامت s در https یا قفل سمت چپ نشان‌دهنده امن بودن ارتباط مشتری با وبسایت

دروازه پرداخت اینترنتی پرداخت الکترونیک سامان

اطلاعات کارت

انتخاب کارت

شماره کارت

رمز اینترنتی

CVV2

تاریخ انقضا

کد امنیتی

تکمیل

ذخیره شماره کارت و تاریخ انقضا در سامانه های پرداخت سامان

ذخیره

پرداخت

اطلاعات پذیرنده

زمان باقیمانده: 05:00

لوگوی شرکت ارائه
 دهنده خدمات پرداخت

جیبی‌مو

کد ترمینال پذیرنده: 10140178

کد پذیرنده: 10112008

نام پذیرنده: نوآوران راهبرد سپهر پارسا

آدرس سایت پذیرنده: jebibmo.com

مبالغ قابل پرداخت (مبلغ): 100,000 ریال

نام و لوگو رسمی فروشگاه
 که از آن خرید می‌کنید.

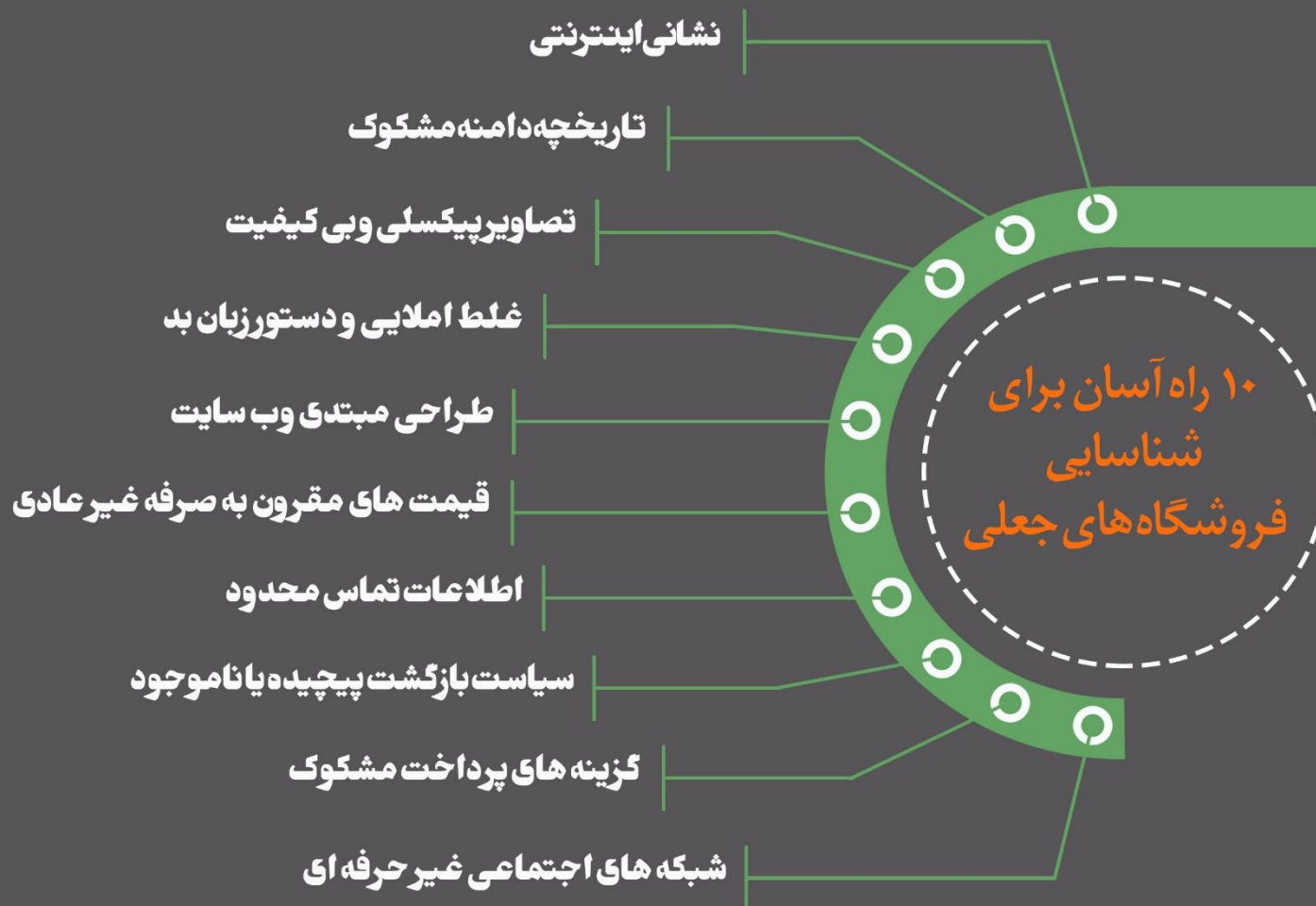
راهبها و نکات امنیتی

در این روش کلاهبرداران با **ساخت فروشگاه اینترنتی** و ارائه اجناس و خدمات با قیمت پایین‌تر و تخفیف‌های جذاب مشتریان را ترغیب به خرید می‌کنند و در مواردی با نام و نشان شرکت‌های معروف سبب جلب اعتماد مشتریان می‌شوند.

برخی از فروشگاه‌های قلبی **به درگاه پرداخت اینترنتی جعلی** متصل هستند و با استفاده از روش ذکر شده در بالا (فیشینگ) اقدام به کلاهبرداری می‌کنند.

در مواردی عملیات پرداخت با استفاده از **واریز کارت به کارت** انجام می‌شود اما پس از واریز به حساب اجناس یا خدمات توافق شده به مشتریان تحویل داده نمی‌شود.







همه وبسایت‌هایی که به صورت قانونی فعالیت می‌کنند ملزم هستند برخی از مجوزهای الکترونیکی را دریافت کنند.



digistyle.com

صاحب امتیاز : نو آوران حمل و نقل چابک ایرانیان

تاریخ اعطا : ۱۳۹۵/۰۸/۰۳

تاریخ اعتبار : معتبر تا تاریخ ۱۴۰۲/۱۰/۲۸



آدرس رسانه بر خط: **digistyle.com**

صاحب امتیاز: نوآوران فن آواره

پست الکترونیکی: **info@digistyle.com**

کد شامد: **4-0-65-700123-2-1**

وضعیت نماد: معتبر از تاریخ ۱۳۹۹/۰۷/۰۲ تا تاریخ ۱۴۰۱/۰۵/۲۷

برای ثبت امتیاز به این تارنما رو اینجا کلیک کنید.

جهت اظهار نظر و یا گزارش تخلف در ارتباط با این تارنما، روی **اینجا** کلیک کنید.

کلاهبرداران اینترنتی با قرار دادن مدارهای مغناطیسی در دستگاه‌های کارتخوان و یا دستگاه خودپرداز بانک اطلاعات کارت بانکی مشتریان را ذخیره و با ساخت کارت جعلی در زمان مناسب حساب بانکی افراد را خالی می‌کنند.



این روش معمولاً با اضافه کردن قطعه سخت افزاری جانبی به دستگاه کارتخوان یا خودپرداز انجام می‌شود و با بررسی فیزیکی قابل تشخیص است.

چگونه گرفتار اسکیمر نشویم؟



دریافت رسید و اطمینان از
اطلاعات درج شده در آن



رمز کارت خود را شخصاً
وارد کنید.



شخصاً به دستگاه کارت
خوان مراجعه کنید.



کارت و رمز آن را در اختیار
دیگران قرار ندهید.



در این روش کلاهبردارن اجناسی را خریداری می‌کنند و **رسید بانکی مشابه** رسیدهای واقعی را برای صاحب اجناس ارسال می‌کنند که هیچ تفاوتی با رسیدهای واقعی ندارد.



اگر صاحب کسب و کار **موجودی حساب** را **بررسی نکند** به راحتی در دام می‌افتد و تصور می‌کند پول به حساب واریز شده است.

چند پیشنهاد برای
جلوگیری از کلاهبرداری
با رسید جعلی



مطمئن‌ترین روش برای
آگاهی از واریز پول، استفاده
از اینترنت بانک و اپلیکیشن
های بانکی است.



در پرداخت‌های شبای پول با
تاخیر واریز می‌شود. تا
اطمینان از دریافت پول،
کالا را نفرستید.



در صورت عجله خریدار و
دسترسی نداشتن به
اینترنت بانک و پیامک، با
مراجعه به بانک از واریز
وجه مطمئن شوید.



اگر می‌خواهید با پیامک از
واریز پول باخبر شوید،
بررسی کنید که پیامک با
سرشماره بانک ارسال شده
باشد. کلاهبردارها می‌توانند
پیامک‌های جعلی هم
بفرستند.





رقم مبلغ جداکننده



تراکنش موفق
در وسط کادر
قرار نگرفته است

کانال
تلگرام

این نوشته و
کادر کشیده
شده است

در این روش کلاهبرداران با قرار دادن **تبلیغات و بنرهای جذاب** در سایت‌ها توجه مشتریان را جلب می‌کنند و با کلیک بر روی بنرها ویروس یا برنامه‌ای بر روی سیستم کاربران نصب می‌شود که می‌تواند اطلاعات موجود بر روی سیستم را ذخیره کند و یا گاهی اوقات با بازکردن صفحه و لینکی در اینترنت صفحات دیگری نیز برخلاف میل افراد باز می‌شوند.

به این ترتیب کلاهبرداران به **اطلاعات خصوصی** و جزئیات حساب‌های شما دسترسی پیدا می‌کنند.

در برخی موارد این اتفاق به **صورت پنهانی رخ نمی‌دهد!** برخی از برنامه‌های رایگان نیز قابلیت ذخیره اطلاعات کاربران را دارند.

برای جلوگیری از این موارد حتماً بر روی سیستم خود **نرم افزارهای ضد ویروس و تروجان و برنامه‌های امنیتی** نصب کنید.



۶ برنامه کاربردی که در گوگل پلی به عنوان **آنتی ویروس** معرفی شده بودند، اطلاعات حساس حدود ۱۵۰۰ کاربر اندروید را به سرقت بردند. پس از شناسایی این نقص، گوگل به سرعت این ۶ **آنتی ویروس** را از پلی استور حذف کرد.



Atom Clean-Booster, Antivirus

Zbynek Adamcik Tools



Antivirus, Super Cleaner

Zbynek Adamcik Tools



Alpha Antivirus, Cleaner

Adelmio Pagnotto Tools



Powerful Cleaner, Antivirus

Adelmio Pagnotto Tools



Center Security - Antivirus

Bingo Like Inc Productivity



Center Security - Antivirus

Bingo Like Inc Productivity

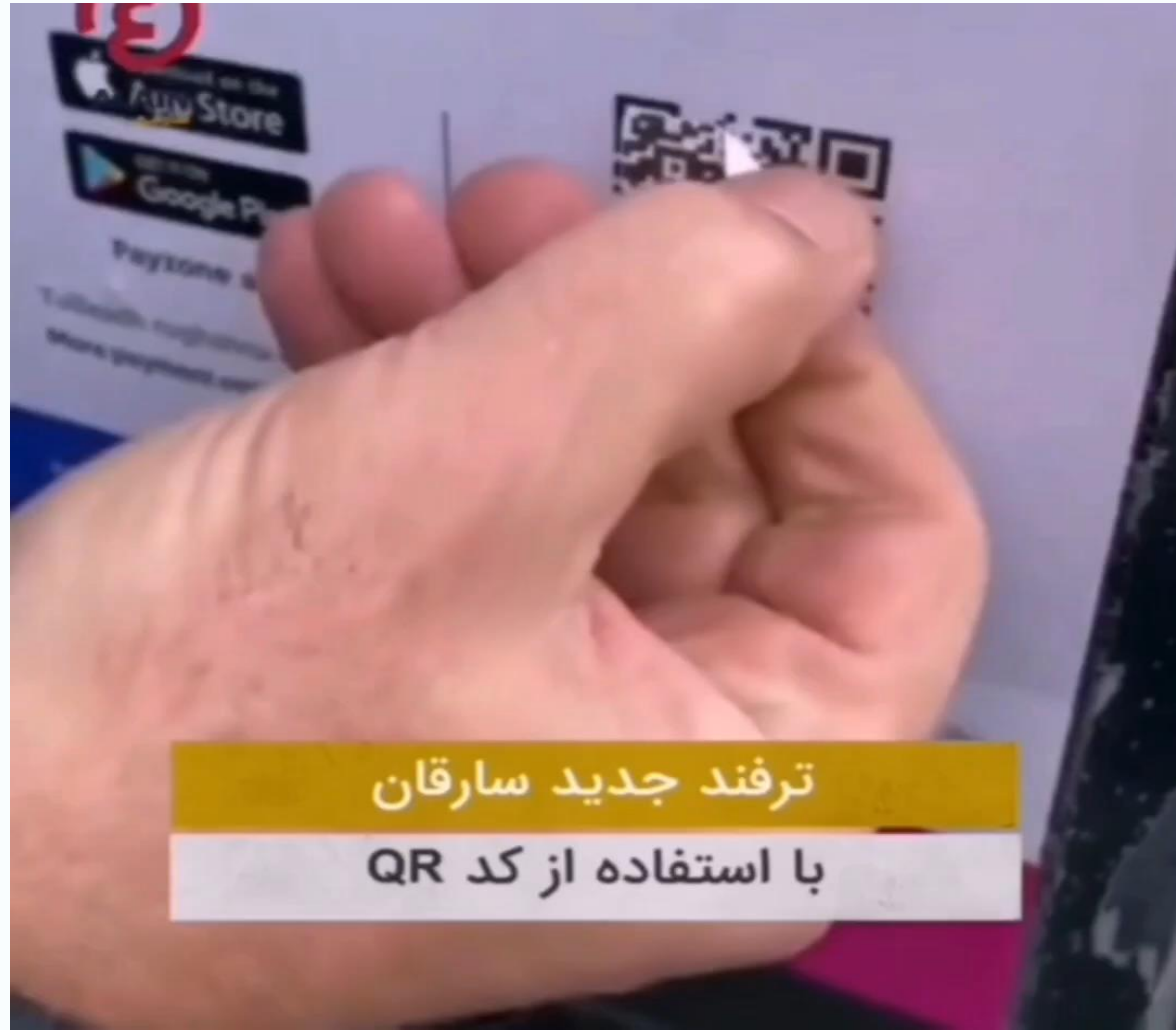
در این روش کلاهبرداران **پیامک** یا **ایمیل** حاوی لینک پرداخت برای پرداخت قبض و را برای افراد ارسال می‌کنند.

کاربران با کلیک بر روی این لینک‌ها به **درگاه‌های جعلی (فیشینگ)** منتقل و اطلاعات آنها سرقت می‌شود یا با ویروس اطلاعات آنها را سرقت می‌کنند.

برای جلوگیری از این روش هرگز **لینک‌های ناشناس** را باز نکنید.







کیو آر کدهایی که می‌زنیم
شاید همیشه امن نباشند!...

بعضی افراد با استفاده از
کدهای جعلی و مخرب، به
اطلاعات شخصی و حساب
های بانکی ما دسترسی پیدا
می‌کنند!...

در یکی از انواع روش‌های کلاهبرداری اینترنتی، کلاهبرداران با **ساخت ایمیل‌های جعلی** **مشابه شرکت‌های معروف و بزرگ با اندکی تغییر در آدرس ایمیل** اقدام به صحبت با مشتریان شرکت‌ها کرده و با آنها از طرف شرکت معامله می‌کنند.

این دسته از کلاهبرداری‌ها معمولاً در کشورهای مختلف انجام می‌شوند و در موارد بسیاری **قابل پیگیری نیستند.**

در بیشتر این کلاهبرداری‌ها **جعل هویت شخص** یا اشخاص نیز صورت می‌گیرد.



در این روش کلاهبرداران با **جمع‌آوری رسیدهای حساب افراد** که در کنار دستگاه‌های خودپرداز رها می‌شوند به بانک‌ها مراجعه می‌کنند.

این افراد با **ارائه مدارک هویتی جعلی** اقدام به دریافت کارت و سرقت از آن می‌کنند.



خالی کردن حساب به بهانه قرعه‌کشی

در این روش کلاهبرداران شماره تماس مشتریان را در سایت‌ها به بهانه **قرعه‌کشی** جمع‌آوری می‌کنند و با آنها تماس می‌گیرند.



یا پیامک‌هایی تحت عنوان **"شما برنده شدید"** ارسال می‌کنند و از کاربران می‌خواهند تا مبلغی را برای ارسال جایزه واریز کنند.

این دسته از کلاهبرداری‌ها در مواردی فقط **واریز هزینه ارسال** هستند اما در مواردی نیز حاوی **لینک درگاه جعلی** هستند.

این روش از انواع روش‌های کلاهبرداری اینترنتی با وجود قدیمی بودن و اطلاع‌رسانی‌های بسیار همچنان افراد زیادی را در دام می‌اندازد.

برخی از **سایت‌های شرط‌بندی** فوتبال و ... مبالغی را تحت عنوان شرط‌بندی از کاربران خود دریافت می‌کنند.

این مبالغ در ابتدا کم و در ادامه بیشتر می‌شوند و پس از مدتی کلاهبرداران سایت را از دسترس خارج می‌کنند و مال باختگان به علت **غیرقانونی بودن** کسب و کار معمولاً شکایت و پیگیری هم نمی‌کنند.



خانه‌های خالی، زمین‌هایی که برای مدتی استفاده نشده‌اند و مواردی از این قبیل **طعمه تبهکاران** هستند.



در این روش کلاهبرداران مواردی را برای مثال یک خانه را با **قیمت و تخفیف چشم‌گیری** بر روی سایت‌های جعلی **فروش** قرار می‌دهند و اقدام به دریافت همه یا بخشی از مبلغ می‌کنند.

این موارد معمولاً با مدارک جعلی به **چندین نفر** فروخته می‌شوند.

کلاهبرداری‌های اینترنتی یکی از چالش‌های جدی در دنیای دیجیتال امروز هستند. آگاهی از روش‌های مختلف کلاهبرداری و راه‌های مقابله با آن‌ها می‌تواند به کاربران کمک کند تا از خطرات احتمالی جلوگیری کنند. استفاده از بهترین درگاه پرداخت اینترنتی و فعال‌سازی رمز دوم پویا از جمله اقداماتی است که می‌تواند امنیت تراکنش‌های آنلاین را افزایش دهد. با رعایت نکات ایمنی و گزارش کلاهبرداری‌ها، می‌توان به کاهش این نوع جرائم کمک کرد و از اطلاعات و سرمایه خود محافظت کرد.