



# دانشتني های ساپیری

مجموعه محتوای پیشگیرانه در حوزه فضای مجازی

## #خرید\_امن

مولف: حامد محمدی سپاسی



# دانستنی‌های سایبری

## جلد ششم

ویراست دوم

حامد محمدی سپاسی





بند هفتم حکم مقام معظم رهبری (مد ظله العالی) در  
دوره دوم تشکیل شورای عالی فضای مجازی

ترویج هنجارها، ارزش‌ها و سبک زندگی اسلامی  
ایرانی و ممانعت از رخنه‌ها و آسیب‌های فرهنگی  
و اجتماعی در این عرصه و مقابله مؤثر با تهاجم  
همه‌جانبه فرهنگی و نیز ارتقای فرهنگ کاربری  
و سواد فضای مجازی جامعه.



بدینوسیله از کلیه همکاران و کارشناسان پیشگیری از جرائم سایبری پلیس فتا استانها که ما را در تهیه و تدوین مجموعه کتاب دانشتهای سایبری پلیس فتا یاری نمودند تقدیر و تشکر می‌کنیم.

از درگاه ایزد منان دوام عزت و سلامت و توفیق روزافزون این عزیزان را خواستاریم.

## فهرست

مقدمه

فصل اول : خرید امن

نماد اعتماد الکترونیکی

در هنگام پرداخت خریدهای اینترنتی از فیلترشکن استفاده نکنید.

مراقب تبلیغات دروغین و اغوا کننده باشید.

دسترسی به اطلاعات تلفن همراه با ارسال پیامک جعلی ابلاغ الکترونیک قضایی

مراقب درگاه‌های جعلی اینترنت بانک باشید

تا حد امکان از پرداخت بیعانه خودداری کنید

خرید از منابع نامعتبر ریسک بالایی دارد

۲۶

چگونه خریدی امن از فضای مجازی داشته باشیم؟

۲۸

جعل اینماد (enamad) و کلاهبرداری از هموطنان

۳۰

کلاهبرداری با اکانت های هک شده

۳۲

آگهی های جعلی در کمین شهروندان

۳۴

نماد اعتماد الکترونیکی جعلی روشی برای جلب اعتماد قربانیان

۳۶

مراقب تبلیغات دروغین مجرمان سایبری در سایت ها واسط باشید

۳۸

کلاهبرداری از طریق اپلیکیشن های رسید ساز

۴۰

اینترنت هدیه ترفندی برای کلاهبرداری از کاربران

۴۲

کلاهبرداری با نرم افزارهای پیام رسان جعلی

## فهرست

۴۴

عدم ارسال کالا یکی از روش های کلاهبرداری

۴۶

چگونه خریدی آنلاین و امن در فضای مجازی داشته باشیم؟

۴۸

حراجی های آنلاین و کلاهبرداری اینترنتی

۵۰

تبلیغات جذاب و البته جعلی در کمین کاربران فضای مجازی

۵۲

شبکه های اجتماعی بستری نا مطمئن برای انجام خرید های اینترنتی

۵۴

تخفیف های ویژه و باورنکردنی شگرد مجرمان سایبری

۵۶

هیچ ارزانی بی علت نیست. پس هوشیار باشید

۵۸

کلاهبرداری اینستاگرامی در پوشش فروش کالا

۶۰

فقط از فروشگاه های مطمئن و دارای مجوز خرید کنید



۶۲

● فعال کردن سامانه پیامکی راهکاری برای ارتقاء امنیت کاربران

۶۴

● عدم ارسال کالا شگرد مجرمان سایبری

۶۶

● مراقب رسید سازهای واریز جعلی باشید

۶۸

● نکات کلیدی در خرید امن آنلاین

۷۰

● کلاهبرداری در سایت‌های درج آگهی

۷۲

● دریافت بیعانه شگردی قدیمی اما رایج

۷۴

● رسیدهای جعلی شگردی برای کلاهبرداری از فروشندگان!

۷۶

● کلاهبرداری‌های اینترنتی از طریق سایت‌های درج آگهی

۷۸

● خرید اینترنتی ایمن چه ویژگی‌هایی دارد؟

۸۰

● رمز دوم پویا راهکاری برای جلوگیری از برداشت غیر مجاز

زندگی در فضای مجازی پر سرعت و پر هیاهو نیازمند برخورداری از مهارت و آگاهی‌های زیادی است. این آگاهی‌ها به خصوص به ما کمک می‌کند تا گرفتار مجرمانی که در کمین سرمایه‌ها و داده‌های ما هستند نشویم.

در این کتاب که به همت مرکز تشخیص و پیشگیری از جرایم سایبری پلیس فتا ناجا تهیه شده است، مجموعه‌ای از هشدارهای پیشگیرانه سایبری است و خواننده می‌تواند به کمک آنها با شیوه‌های مجرمانه سایبری و راهکارهای پیشگیری از آنها آشنا شود. مطالب این کتاب متناسب با موضوع در قالب عکس نوشته و توضیحات تکمیلی جمع‌آوری شده است و این به خواننده کمک می‌کند تا بتواند خیلی سریع و در قالب متن‌های کوتاه با هشدار و راهکار پیشگیری از آن که ناشی از تجربیات کارشناسان پلیس فتا است آشنا شود.

این مجموعه با رویکرد مدیریت دانش پیشگیری از جرم کارشناسان پلیس فتا تهیه شده است، اما خواندن آن را به کلیه کاربران فضای مجازی فارغ از هر سطح تحصیلات و مهارت توصیه می‌شود.

رئیس مرکز تشخیص و پیشگیری از جرایم سایبری پلیس فتا فراجا

سرهنگ دوم علی محمد رجبی



[www.cyberpolice.ir](http://www.cyberpolice.ir)

دانشی‌های سایبری



# خرید اینترنتی امن





پلیس فضای تولید و تبادل اطلاعات ناجا  
www.cyberpolice.ir



## #خرید\_امن نماد اعتماد الکترونیکی

خریدهای اینترنتی خود را تنها از فروشگاه های معتبر که دارای سایت با نماد اعتماد الکترونیکی هستند انجام دهید.



برای خریدی امن، حتما از فروشگاه های دارای نماد اعتماد الکترونیکی استفاده کنید. خرید از فروشگاه های دارای نماد این اطمینان را به خریدار می دهد که فروشگاه مذکور اقدام به ارائه اجناس مجاز نموده و حتی در صورت کلاهبرداری نیز قابلیت پیگیری بسیار آسان تر خواهد بود. خرید از فروشگاه هایی که فقط در شبکه های اجتماعی فعال هستند و اینماد(Enamad) ندارند، می تواند زمینه سرقت اطلاعات بانکی کاربران را فراهم آورد. بنابراین هموطنان عزیز باید قبل از پرداخت هرگونه وجه در هر قالب(بیعانه، پیش پرداخت، واریز کامل وجه و ...) از اصالت فروشگاه اطمینان حاصل کرده و پرداخت وجه را به درب منزل موکول نمایند.

بنابراین کسانی که خریده های خود را به صورت آنلاین انجام می دهند باید به خاطر داشته باشند:

خرید از فروشگاه های دارای نماد اعتماد الکترونیکی، امنیت آنان را بالا خواهد برد. با کلیک بر روی تصویر این نماد وارد سایت [enamad.ir](http://enamad.ir) شده و مشخصات فروشگاه را می توانید بررسی کنید.

“#خرید امن”

در  
پرداخت  
خریدهای اینترنتی  
فیلتر شکن  
را  
خاموش  
کنید!

استفاده از فیلتر شکن باعث  
می‌شود تا اطلاعات بانکی  
شما در اختیار  
شخص دیگری قرار بگیرد..



www.cyberpolice.ir



## در هنگام پرداخت خریدهای اینترنتی از فیلترشکن استفاده نکنید.

از آنجایی که در هنگام نصب برخی از فیلتر شکن ها، شاهد موارد تبلیغاتی و گاهی اوقات نصب برنامه های ناخواسته دیگر می باشیم، لذا ممکن است اطلاعات کاربران را کپی و به سرقت ببرند. بنابراین توصیه می شود شهروندان از نصب و استفاده از فیلترشکن ها خودداری کنند. هموطنان گرامی این نکته را به خاطر داشته باشند که سایت های فیلتر شده قطعاً دارای موارد مجرمانه بوده و به همین دلیل در کارگروه تعیین مصادیق مجرمانه فیلتر شده اند. بنابراین استفاده از این سایت ها با ریسک بالایی همراه خواهد بود. این مورد در سایت های فروشگاههای و درگاه های جعلی نمود بیشتری پیدا می کند چرا که به محض وارد کردن اطلاعات بانکی، مجرمان سایبری اقدام به برداشت غیر مجاز از حساب آنان خواهند کرد. پس اگر برای انجام کارهای بانکی از vpn یا فیلتر شکن استفاده نکنیم رفتار سایت های فیلتر شده نخواهیم شد. بنابراین به هموطنان عزیز توصیه می شود: بهتر است برای انجام خریدها و انجام امور بانکی خود به آدرس درگاه های بانکی توجه کرده و سعی کنند خرید های خود را از فروشگاه های معتبر و دارای نماد اعتماد الکترونیکی انجام دهند.

**VPN**  
Connections

# مراقب تپاخات دروغین وانرا ککنده کلهپردارن در نرم افزارهای واسط خرید و فروش کالای دسته دوم باشین



به کاربران توصیه می‌شود جهت تجربه خریدی امن از پرداخت بیعانه به فروشندگان برای خرید کالا خودداری کنند.





## مراقب تبلیغات دروغین و اغوا کننده باشید.

مراقب تبلیغات دروغین و اغوا کننده کلاهبردارن در نرم افزارهای واسط خرید و فروش کالای دسته دوم باشید.

کلاهبرداران سایبری با ارائه تبلیغات دروغین و اغوا کننده و بهره بردن از شیوه های مختلف مهندسی اجتماعی در فضای مجازی و بخصوص سایت ها و یا اپلیکیشن های واسط خرید و فروش کالای دسته دوم به دنبال جلب افراد و کلاهبرداری از آنها هستند. این افراد با ارائه قیمت هایی پایینتر و یا جمله هایی جذاب سعی در ارائه اجناسی با کیفیت پایین داشته و کاربران را ترغیب به انجام خواسته های خود می نمایند. این افراد در ازای حفظ کالا خواستار دریافت بیعانه و پیش پرداخت می شوند. وجه اشتراک بسیاری از پرونده های تشکیل شده در پلیس فتا، پرداخت بیعانه و پیش پرداخت و عدم پاسخگویی فرد فروشنده است. در هنگام خرید های آنلاین در صورت امکان پرداخت وجه را به صورت حضوری و درب منزل انجام دهید.

همچنین پلیس فتا به هموطنان گرامی توصیه می کند، جهت تجربه خریدی امن، از پرداخت بیعانه به فروشندگان برای خرید کالا خودداری کند.



پلیس فضای تولید و تبادل اطلاعات ناجا

پیامک جعلی سامانه ثنا

# هک تلفن همراه شما

کلاهبرداران اینترنتی با ارسال پیامک جعلی ابلاغ الکترونیک قضایی  
تلفن همراه شما را هک و از جانب شما پیامک ارسال می‌کنند.

کاربر گرامی  
علیه شما شکایتی  
در سامانه ثنا ثبت شده است



**هشدار  
مهم و فوری**

## دسترسی به اطلاعات تلفن همراه با ارسال پیامک جعلی ابلاغ الکترونیک قضایی



اخیراً شاهد ارسال پیامک‌هایی با محتوایی همچون ابلاغ الکترونیک قضایی، پرداخت یارانه، سامانه سجام و... به شهروندان می‌باشیم. این پیامک‌ها حاوی لینک‌هایی هستند که از کاربران درخواست می‌کند جهت انجام ادامه کار، اپلیکیشن مربوطه را روی تلفن همراه خود نصب نمایند. این پیامک‌ها معمولاً تحت عنوان سازمان‌ها و ارگان‌های دولتی ارسال تا بتوانند اعتماد کاربران را جلب نمایند. از آنجایی که سازمان‌ها و ارگان‌های دولتی برای ارسال پیامک از سرشماره‌های مخصوص استفاده می‌کنند لذا عمده پیامک‌های ارسالی جعلی بوده و تنها با هدف کلاهبرداری طراحی شده‌اند.

متأسفانه برخی از شهروندان از این سامانه‌ها و نحوه فعالیت آن‌ها آگاهی کافی ندارند لذا در دام کلاهبرداران اینترنتی گرفتار شده و تلفن همراه آنها عاملی برای انجام جرم می‌شود. مجرمان سایبری در مرحله بعد از طریق سیم کارت و تلفن همراه فرد قربانی، اقدام به ارسال پیامک برای مخاطبین وی ارسال کرده و از آنها درخواست واریز وجه دارند. شهروندان عزیز توجه داشته باشند پیامک‌های ارسال از سوی قوه قضائیه فاقد لینک بوده و برای پیگیری شکوائیه نیازی به واریز هیچ‌گونه وجهی نمی‌باشد.



## مراقب درگاه های جعلی اینترنت بانک باشید



ساده ترین راه برای دسترسی به اینترنت بانک، جستجو در موتورهای جستجوگر اینترنتی است. این در حالی است که سایت مورد بازدید می تواند جعلی و با هدف سرقت اطلاعات کاربران طراحی شده باشد. بنابراین استفاده کنندگان از اینترنت بانک باید در فرم های لاگین به آدرس (url) دقت و توجه ویژه داشته باشند. نکته اینکه سایت های جعلی می توانند دارای آدرسی شبیه به سایت اصلی داشته باشند که به دلیل شباهت سایت اصلی با جعلی (فیشینگ)، با ورود به سایت های جعلی، اطلاعات حساب کاربری شامل نام کاربری، رمز ورود و سایر اطلاعات بانکی آنها توسط مجرمان به سرقت می رود. بنابراین باید آدرس اینترنت بانک از سایت رسمی بانک مربوطه دریافت و توسط کاربر نوشته شود تا احتمال گرفتار شدن در دام مجرمان کاهش پیدا کند. شهروندان محترم حتماً آدرس اینترنتی بانک مورد نظر خود را به خاطر داشته و از کلیک کردن بر روی لینک های ارائه شده در شبکه های اجتماعی و سایت های نامعتبر خودداری نمایند.

همچنین آدرس معتبر ورود به اینترنت بانک های رسمی کشور در سایت رسمی پلیس فتا به نشانی <https://cyberpolice.ir/links> (قسمت آدرس اینترنت بانک ها) قرار گرفته است که هموطنان به راحتی و با اطمینان می توانند از آن استفاده کنند.



پلیس فضای تولید و تبادل اطلاعات ناجا



# پرداخت بیعانه ممنوع

تا کالایی را از نزدیک ندیده‌اید به هیچ وجه مبلغی را به عنوان ودیعه پرداخت نکنید و بعد از دریافت کالا و اطمینان از کیفیت و قیمت آن، اقدام به پرداخت وجه نمایید.



## تا حد امکان از پرداخت بیعانه خودداری کنید

یکی از مهمترین شگردهای رایج مجرمان سایبری، سوءاستفاده از اعتماد قربانیان و بهره بردن از شیوه های مهندسی اجتماعی می باشد. این افراد سعی دارند با استفاده از جملات جذاب و اغوا کننده، اعتماد کاربران را جلب و آنان را ترغیب به انجام خواسته های خود نمایند. یکی از مهمترین روش های رایج ثبت آگهی های جعلی در سایت های درج آگهی آنلاین بوده که پس از جلب اعتماد کاربر از وی درخواست واریز بیعانه و پیش پرداخت به عنوان مختلف می نمایند. این مجرمان پس از دریافت بیعانه دیگر پاسخگو نخواهند بود.

هموطنان گرامی در نظر داشته باشند:

- در صورت پرداخت بیعانه و پیش پرداخت هیچگونه تضمینی برای ارسال کالا وجود نخواهد داشت.
- پرداخت وجه را به بعد از روئیت کالا موکول کنید.
- در صورت خرید کالاهای دیجیتالی حتماً فاکتور فروش را از فروشنده درخواست نمایید تا در صورت وجود هر مشکل (سرقتی بودن و...) مسئولیتی متوجه شما نباشد.

# صفحات و کانال‌هایی که احتمال کلاهبرداری در آنها بالاست

- ▶ صفحه به تازگی باز شده است
- ▶ دارای آدرس و تلفن مشخصی نیست
- ▶ اکثر پست‌ها در یک تاریخ بارگزاری شده‌اند
- ▶ محصولات را با قیمت نامعقولی عرضه می‌کنند
- ▶ محصولاتی که در بازار وجود ندارد را تبلیغ می‌کنند
- ▶ انتقاد کاربران از عدم تحویل و کلاهبرداری در کامنت‌ها



#خریدارمان



## خرید از منابع نامعتبر ریسک بالایی دارد

یکی از مهمترین توصیه‌های پلیس فتا این است که «از فروشگاه‌های معتبر خرید نمایید». با این کار احتمال وقوع کلاهبرداری و سوءاستفاده کمتر خواهد شد.

برخی از مجرمان سایبری با ایجاد کانال‌ها و صفحات جعلی فروشگاه‌های اقدام به سوءاستفاده و کلاهبرداری از شهروندان، ارائه اجناس و کالاهای غیر مجاز و ممنوعه می‌کنند.

برخی از مشخصات صفحات فروشگاه‌های جعلی به شرح زیر می‌باشد:

- ۱- صفحه به تازگی باز شده است.
- ۲- دارای آدرس و تلفن مشخصی نیست.
- ۳- اکثر پست‌ها در یک تاریخ بارگزاری شده‌اند.
- ۴- محصولات را با قیمت‌هایی نامعقول عرضه می‌کنند.
- ۵- انتقاد کاربران از عدم تحویل و کلاهبرداری در کامنت‌ها وجود ندارد.
- ۶- محصولات غیر مجاز و ممنوعه را تبلیغ و به فروش می‌رسانند.



50%  
تخفیف ویژه

در هنگام خرید از فروشگاه‌ها در شبکه‌های اجتماعی همانند اینستاگرام، هیچ‌گاه فریب تبلیغات اغوا کننده آن‌ها را نخورید و حتماً از فروشگاه‌هایی خرید کنید که دارای نماد اعتماد هستند

هیچ‌گاه تعداد دنبال کننده یک فروشگاه در شبکه‌های اجتماعی دلیلی برای اصالت آن فروشگاه نخواهد بود

#خرید\_امن



## چگونه خریدی امن از فضای مجازی داشته باشیم؟

هیچ‌گاه فریب تبلیغات اغوا کننده صفحات فروشگاه‌های در فضای مجازی را نخورید و حتماً از فروشگاه‌هایی خرید کنید که دارای نماد اعتماد الکترونیکی و سایر مجوزها باشند. این سایت‌ها معمولاً محصولات مجاز را ارائه کرده و دارای اعتبار لازم هستند. کاربران می‌توانند با مراجعه به سایت [namad.ir](http://namad.ir) لیست فروشگاه‌های دارای نماد را مشاهده نمایند.

خرید از فروشگاه‌های دارای نماد این اطمینان را به خریدار می‌دهد که فروشگاه مذکور اقدام به ارائه اجناس مجاز نموده و حتی در صورت کلاهبرداری نیز قابلیت پیگیری بسیار آسان‌تر خواهد بود.

خرید از فروشگاه‌هایی که فقط در شبکه‌های اجتماعی فعال هستند و اینماد (Enamad) ندارند، می‌تواند زمینه سرقت اطلاعات بانکی کاربران را فراهم آورد. بنابراین قبل از پرداخت هرگونه وجه در هر قالب (بیعانه، پیش‌پرداخت، واریز کامل وجه و ...) از اصالت فروشگاه اطمینان حاصل کرده و پرداخت وجه را به درب منزل موکول نمایند.

این موضوع را نیز به یاد داشته باشید که هیچ‌گاه تعداد دنبال‌کننده یک فروشگاه در شبکه‌های اجتماعی دلیلی برای اصالت آن فروشگاه نخواهد بود.



# خرید-امن

# کلاهبرداری با درج نماد اعتماد الکترونیک جعلی

افراد سودجو با راه اندازی سایتهای فروش کالا و درج نشان جعلی اینماد، اقدام به کلاهبرداری از شهروندان می‌کنند





## جعل اینماد (enamad) و کلاهبرداری از هموطنان

برخی از مجرمان سایبری با راه اندازی سایت‌های فروشگاهی و درج نشان جعلی اینماد به دنبال جلب اعتماد کاربران و در نهایت کلاهبرداری از آنان می‌باشند. این افراد با طراحی لوگو که از نظر ظاهری کاملاً با لوگو اینماد شبیه است قصد فریب کاربران را داشته و با درج این لوگو در صفحه اول فروشگاه خود سعی دارند اعتماد خریداران را جلب و در ادامه از حساب آنان برداشت غیر مجاز داشته باشند. با توجه به اینکه جعل کردن نماد اعتماد الکترونیکی از قبل نیز پیش بینی شده، لذا مرکز توسعه و تجارت الکترونیکی برای جلوگیری از سوء استفاده این افراد اقدام به ارائه راه کار مناسبی نموده است.

در این روش بعد از کلیک کردن روی لوگو اینماد به صفحه ای لینک داده خواهید شد که مجوز فروشگاه مربوطه به همراه سابقه ای مختصر از دامنه و صاحب امتیاز این فروشگاه قابل مشاهده خواهد بود.

نکته اینکه صفحه باز شده تصویر نیست و در صفحه اصلی مرورگر باز خواهد شد و این صفحه باید با آدرس [enamad.ir](http://enamad.ir) آغاز شده باشد و آدرس اینترنتی (URL) سایت فروشگاه یا بازار الکترونیک با آدرسی که در این صفحه معرفی می‌شود باید یکسان باشد.

همچنین لیست تمامی فروشگاه های دارای نماد در این سایت قابل دریافت خواهند بود.

# کلاهبرداری با اکانت‌های هک شده

پیش از هرگونه واریز وجه  
از صحت پیام‌های ارسال  
شده اطمینان پیدا کنید.

کاربران در صورت دریافت هرگونه پیامک  
از مخاطبان و آشنایان خود مبنی بر  
درخواست کمک نقدی به عنوان قرض،  
ابتدا موضوع را بررسی کرده و با تماس با  
وی و پرس و جو از اطرافیان، از صحت و  
سقم موضوع مطمئن شوند و هیچ‌گاه با  
عجله و شتاب و بدون تحقیق در مورد  
موضوع اقدام به واریز وجه نکنند.





## کلاهبرداری با اکانت های هک شده

دسترسی غیرمجاز به حساب کاربری دیگران و سوء استفاده از آن، یکی از روش هایی است که به تازگی مورد استفاده مجرمان سایبری قرار گرفته و این افراد با استفاده از این روش به دنبال کلاهبرداری از اقوام و آشنایان فرد هک شده می باشند. این افراد با دسترسی غیر مجاز به حساب کاربری قربانیان و دسترسی به دفترچه تلفن آنها سعی می کنند با برقراری ارتباط با مخاطبین از آنها درخواست واریز وجه نمایند. عمده کلاهبرداری های صورت گرفته متعلق به دوستان، آشنایان و اقدام فرد قربانی است. با توجه به شناختی که بین این افراد با فرد قربانی وجود دارد لذا برخی از دوستان وی به درخواست او اقدام به واریز وجه درخواستی می نمایند.

بنابراین لازم است هموطنان گرامی در گام نخست امنیت خود در فضای مجازی را بالا برده و با انتخاب رمزهای عبور قوی و همچنین عدم مراجعه به لینک های اعلامی در شبکه های اجتماعی امنیت خود و دوستان خود را ارتقاء دهند.

در گام بعد نیز قبل از هرگونه واریز وجه از صحت پیام های ارسال شده اطمینان پیدا کرده و در صورت دریافت هرگونه پیامک از مخاطبان و آشنایان خود مبنی بر درخواست کمک نقدی به عنوان قرض، ابتدا موضوع را بررسی و با تماس با وی و پرس و جو از اطرافیان، از صحت و سقم موضوع مطمئن شوید و هیچگاه با عجله و شتاب و بدون تحقیق در مورد موضوع اقدام به واریز وجه نکنید.



# آگهی های جعلی در کمین شهروندان



به سادگی فریب وعده های پوچ و تبلیغات اغواکننده کلاهبرداران را نخورید.



قبل از رویت و اطمینان از اصالت و مدارک کالا اقدام به پرداخت بیعانه نکنید.



کاربران حتما در خصوص صحت هویت فرد آگهی دهنده بررسی های لازم را صورت دهند.



برای خرید حتما از فروشگاه هایی که دارای نماد الکترونیکی هستند اقدام کنید.



## آگهی‌های جعلی در کمین شهروندان



برخی از افراد سودجو با سوءاستفاده از تبلیغات و آگهی‌های تبلیغاتی به دنبال عملی کردن اهداف مجرمانه خود می‌باشند. استفاده از جملات جذاب و اغوا کننده و ارائه قیمت‌هایی پایینتر از عرف بازار در تبلیغات و ارائه محصولات غیر مجاز، فاقد کیفیت و... از مهمترین روش‌های کلاهبرداری از کاربران می‌باشد.

در همین راستا در مواجهه با آگهی‌های تبلیغاتی دقت و توجه بیشتری نیاز است و موارد زیر را در نظر بگیرید:

- ۱- به سادگی فریب وعده‌های پوچ و تبلیغات اغواکننده کلاهبرداران را نخورید.
- ۲- قبل از رویت و اطمینان از اصالت و مدارک کالا اقدام به پرداخت بیعانه نکنید.
- ۳- حتما در خصوص صحت هویت فرد آگهی دهنده بررسی‌های لازم را صورت دهند.
- ۴- برای خرید حتما از فروشگاه‌هایی که دارای نماد الکترونیکی هستند اقدام کنید.





پلیس فضای تولید و تبادل اطلاعات ناجا



اصالت نماد اعتماد

الکترونیکی  
را چک کنید.

فروشگاه های اینترنتی دارای نماد اعتماد را

از وب سایت **Enamad.ir** استعلام بگیرید.

فروشگاه های جعلی فقط تصویری از نماد اعتماد در وب سایت خود درج می کنند. و یا اینکه شما را به لینک جعلی سامانه نماد اعتماد هدایت می کنند.



#خرید\_امن

WWW.CYBERPOLICE.IR

## نماد اعتماد الکترونیکی جعلی روشی برای جلب اعتماد قربانیان

نماد اعتماد الکترونیکی مجوزی است که به کسب و کارهای اینترنتی که دارای فعالیت مجاز بوده اعطا می‌شود. مرکز توسعه و تجارت الکترونیکی به عنوان متولی اعطای این‌نماد با هدف قانونمند کردن و چارچوب دهی به فعالیت آنها در فضای مجازی اقدام به دادن مجوز فعالیت سایت های فروشگاههای تحت عنوان نماد اعتماد الکترونیکی (این‌نماد) نموده است. نماد اعتماد الکترونیکی به شکل یک لوگو در وب سایت‌هایی که از نظر قانونی فعالیت آنان مورد تأیید است درج و در معرض دید عموم قرار گرفته است. در یکی از روش های مجرمانه، برخی از افراد سودجو با شبیه سازی و جعل این لوگو و راه اندازی کسب و کارهای اینترنتی جعلی (فروشگاه های آنلاین و پیج های فروشگاههای در شبکه های اجتماعی) اقدام به کلاهبرداری می کنند. هموطنان گرامی توجه داشته باشند هنگام خرید اینترنتی حتما اصالت نماد اعتماد الکترونیکی را در وب سایت [enamad.ir](http://enamad.ir) بررسی کنند. هنگام کلیک روی نماد اعتماد در وب سایت فروشگاه بایستی یک لینک که حاوی اطلاعات فروشگاه است نمایش داده شود و حتماً با آدرس [enamad.ir](http://enamad.ir) آغاز شده باشد و آدرس (URL) فروشگاههای که در صفحه نماد اعتماد مجوز دارد با آدرس اینترنتی سایت فروشگاه اینترنتی مدنظر یکسان باشد.

# مراقب تبلیغات دروغین و یا ارائه قیمت‌های پایین در سایت‌ها و اپلیکیشن‌های واسط باشید



کلاهبرداران سایبری با ارائه تبلیغات دروغین و یا ارائه قیمت‌های پایین در سایت‌ها و اپلیکیشن‌های واسط به دنبال جلب افراد و کلاهبرداری از آنها هستند.



www.cyberpolice.ir

پلیس فضای تولید و تبادل اطلاعات ناجا

## چگونه یک خرید اینترنتی امن داشته باشیم؟

1. از سایت‌های معتبر خرید کنیم.
2. بعد از دریافت محصول و اطمینان از صحت آن مبلغ را پرداخت کنیم.
3. از سایت‌هایی با نمایندگی اعتماد الکترونیکی خرید کنیم.
4. از پرداخت هرگونه بیعانه خودداری کنیم.



## مراقب تبلیغات دروغین مجرمان سایبری در سایت ها واسط باشید

مجرمان سایبری با ارائه تبلیغات دروغین و جعلی و ارائه قیمت های پایین و باور نکردنی در سایت ها و اپلیکیشن های واسط به دنبال جلب اعتماد کاربران و ترغیب آنها به انجام خواسته های خود و در نهایت سرقت اطلاعات و کلاهبرداری از آنان خواهند بود.

در این شگرد معمولاً پس از جلب اعتماد کاربران از فرد قربانی درخواست مبلغی تحت عنوان بیعانه و پیش پرداخت می نمایند. در گام بعدی و پس از دریافت بیعانه دیگر پاسخو نمی باشند. در این روش معمولاً مبلغی پایین درخواست تا قربانی به علت عدم مقرون به صرفه بودن از طرح شکایت خودداری نماید.

حال این سوال پیش می آید که چگونه یک خرید اینترنتی امن داشته باشیم؟ در پاسخ می توان گفت: هموطنان گرامی باید در هنگام خرید های آنلاین نهایت دقت و حساسیت را داشته و موارد زیر را در نظر بگیرند:

۱. از سایت های معتبر خرید کنیم.
۲. بعد از دریافت محصول و اطمینان از صحت آن مبلغ را پرداخت کنیم.
۳. از سایت هایی با نماد اعتماد الکترونیکی خرید کنیم.
۴. از پرداخت هرگونه بیعانه خودداری کنیم.
۵. پس از پرداخت حساب بانکی خود را چک کنیم.



# اپلیکیشن‌های رسیدساز

مجرمین سایبری با استفاده از اپلیکیشن‌های رسیدساز به دنبال کلاهبرداری از شهروندان هستند

**سرویس دریافت پیامک بانکی خود را فعال کنید**



نرم افزارها و اپلیکیشن‌های مختلف رسیدساز یکی از ترفندهای جدید مجرمان سایبری برای کلاهبرداری از فروشندگان در سایت‌های واسطه‌گرای اینترنتی است.

برخی از فروشگاه‌های اینترنتی در شبکه‌های اجتماعی نیز با انتشار تصاویر فیش‌های واریزی جعلی سعی در جلب اعتماد کاربران دارند که نباید فریب اینگونه تبلیغات را خورد.



## کلاهبرداری از طریق اپلیکیشن‌های رسید ساز



نرم افزارهای رسیدساز یکی از جدیدترین ترفندهای مجرمان سایبری برای کلاهبرداری از فروشندگان می باشد. افراد سودجو بعد از انتخاب و خرید کالا اقدام به پرداخت وجه به صورت اینترنتی نموده و در ادامه با ارائه رسید دیجیتالی و نشان دادن به فروشنده ادعای پرداخت وجه را دارند. در حالت معمول رسید پرداخت به نشانه پرداخت شدن وجه دارد اما با استفاده از برنامه های رسید ساز می توان این رسید ها را به راحتی جعل کرده و با وارد کردن شماره کارت بانکی فروشنده ادعای پرداخت وجه را داشت.

- فعال کردن سرویس پیامک بانکی یکی از ساده‌ترین روش‌های جلوگیری از اینگونه از کلاهبرداری است.

از دیگر شگردهای مجرمانه می توان به ارائه رسید های جعلی توسط برخی از فروشگاه‌های اینترنتی بخصوص پیچ های فعال در شبکه های اجتماعی برای جلب اعتماد سایر کاربران و ترغیب آنها به خرید اشاره کرد.

ارائه تصاویر متعدد فیش‌های واریزی جعلی تحت عنوان خریدهای انجام شده توسط مشتریان، تنها با هدف کلاهبرداری تهیه شده است.

فعال کردن پیامک بانکی و همچنین خرید کردن از فروشگاه های معتبر می تواند امنیت حساب بانکی شما را افزایش دهد.



پلیس فضای تولید و تبادل اطلاعات ناجا  
WWW.CYBERPOLICE.IR



12 کیک اینترنت یکماهه  
برای همه اپراتورها  
ویژه بویس در خانه بمانیم

بمناسبت  
ستاد مقابله با کرونا از وزارت  
ارتباطات درخواست کرد تا  
بسته اینترنتی ویژه جهت در  
خانه بمانیم تامین کند تا فقط  
با پرداخت 2 هزار تومان 12 کیک  
اینترنت یکماهه برای همه  
اپراتور ها این بسته برای تمام  
کاربران ایرانی فعال سازی  
شود

جهت فعال سازی 12 کیک  
اینترنت یکماهه لینک زیر را  
بالا بکشید و شماره خودتون  
رو وارد

هشماره  
کد این  
شماره دور

## کلاهبرداری با ترغیب اینترنت هدیه

به هیچ وجه به لینک‌های ارسالی در کانال‌ها و شبکه‌های اجتماعی با عنوان ثبت‌نام و دریافت اینترنت رایگان توجه نکنید، بیشتر این لینک‌ها جعلی می‌باشند.

## اینترنت هدیه ترفندی برای کلاهبرداری از کاربران



در مناسبت‌های خاص مانند ایام کرونا مجرمان سایبری به بهانه اینترنت رایگان کاربران را با لینک‌های آلوده به درگاه‌های پرداخت جعلی یا نصب برنامه‌های برنامه‌های موبایلی آلوده هدایت می‌کنند.

به هیچ وجه تبلیغات صورت گرفته در فضای مجازی را جدی نگرفته و به لینک‌های ارسالی در کانال‌ها و شبکه‌های اجتماعی با عنوان ثبت نام و دریافت اینترنت رایگان توجه نکنید، چرا که بیشتر لینک‌های ارسال شده جعلی می‌باشد.

# کلاهبرداری در نرم افزار های پیام رسان فضای مجازی



در این روش کلاهبرداری، لینکی به همراه پیام برای کاربران ارسال می‌شود و از افراد خواسته می‌شود که روی آن کلیک کنند. با توجه به اینکه لینک ارسالی آلوده به بدافزار است شهروندان در صورتی که روی لینک مذکور کلیک کنند، بلافاصله تمامی اطلاعات موجود در تلفن همراه از جمله اطلاعات هویتی و بانکی ذخیره شده و غیره در دسترس مجرم قرار می‌گیرد.

**از کلیک روی لینک‌های ناشناس خودداری کرده و این**

**موارد را در سایت پلیس فتا به آدرس [www.CYBERPOLICE.IR](http://www.CYBERPOLICE.IR)**

**در بخش گزارش‌های مردمی ثبت کنید.**



www.cyberpolice.ir

پلیس فضای تولید و تبادل اطلاعات ناجا

## کلاهبرداری با نرم افزارهای پیام رسان جعلی



نقش بدافزارها در انجام جرائم سایبری را نمی توان نادیده گرفت. همواره مجرمین با طراحی بدافزار به دنبال سوءاستفاده و انجام خواسته های مجرمانه خود بوده اند و امروزه این روند رو به رشد می باشد. از آنجایی که کسب منافع مالی همچنان مهمترین انگیزه مجرمان سایبری به شمار می رود لذا بسیاری از بدافزارهای طراحی شده نیز این هدف را دنبال می کنند. این بدافزارها در قالب فایل های ضمیمه و یا لینک های جعلی به سیستم های قربانیان نفوذ می کنند. از جمله مواردی که رو به افزایش بوده و در این ایام بیشتر مورد استفاده مجرمان قرار گرفته بهره بردن از اپلیکیشن های تلفن همراه و نفوذ بدافزار به دستگاه هوشمند فرد قربانی است.

در این روش از کلاهبرداری، لینکی به همراه پیام برای کاربران ارسال می شود و از وی خواسته می شود روی آن کلیک و نرم افزار مربوطه را نصب نماید. با توجه به اینکه نرم افزار آلوده به بدافزار است در صورت نصب آن، تمامی اطلاعات موجود در تلفن همراه از جمله اطلاعات هویتی و پیامک های رمز عبور در دسترس مجرم قرار می گیرد.

بنابراین بسیار مهم است تا کاربران از کلیک کردن بر روی لینک های ناشناس و نصب برنامه های موبایلی غیر امن خودداری کرده و این موارد را در سایت پلیس فتا به آدرس [www.CYBERPOLICE.IR](http://www.CYBERPOLICE.IR) در بخش گزارش های مردمی گزارش کنند.



خرید امن

## کلاهبرداری با عدم ارسال کالا

کلاهبرداران با ایجاد صفحات فروشگاه‌های جعلی در شبکه‌های اجتماعی کاربران را فریب داده و پس از خرید و واریز وجه از سوی شهروندان کالایی را برای آنها ارسال نمی‌کنند و هیچ‌گونه پاسخی به خریدار نمی‌دهند، لذا توصیه می‌کنیم از کسانی خرید نمایانید که سایت فروش معتبر و همچنین نماد اعتماد الکترونیکی دیجیتال داشته باشند.



پلیس فضای تولید و تبادل اطلاعات ناجا

## عدم ارسال کالا یکی از روش‌های کلاهبرداری



متأسفانه برخی از افراد سودجو و کلاهبردار نیز از این موقعیت سوءاستفاده کرده و با برپایی پیج‌های فروشگاهی جعلی در شبکه‌های اجتماعی به دنبال سوءاستفاده از کاربران می‌باشند. این افراد از شیوه و روش‌های مختلفی برای کلاهبرداری استفاده می‌کنند که مهمترین آنها دریافت بیعانه و عدم ارسال کالا می‌باشد. این افراد با استفاده از جملات جذاب و تخفیف‌های بالا کاربران را ترغیب به انجام خواسته‌های خود می‌کنند که مهمترین خواسته آنها واریز مبلغی تحت عنوان بیعانه می‌باشد. این افراد معمولاً مبلغی پایین را به عنوان بیعانه درخواست تا شکایت و پیگیری آن مقرون به صرفه نباشد. البته گروهی دیگر از مجرمان با استفاده از سیم کارت‌ها و شماره حساب‌های فاقد هویت اقدام به کلاهبرداری می‌کنند.

بنابراین توصیه می‌کنیم خرید‌های اینترنتی خود را از وب‌سایت‌های معتبر و دارای مجوز انجام داده و تا حد امکان سعی کنید به تبلیغات صورت گرفته در پیج‌های مختلف در شبکه‌های اجتماعی توجه نکرده و از کلیک کردن بر روی لینک‌های اعلامی خودداری نمایید.

# چگونه خریدی آنلاین و ایمن انجام دهیم

# خرید امن

۱ اعتبار فروشگاه اینترنتی  
را بررسی کنید

۲ مراقب صفحات و درگاه‌های  
پرداخت جعلی باشید

۳ از یک کارت بانکی مجزا برای  
پرداخت آنلاین استفاده کنید

۴ اپلیکیشن‌های فروشگاه‌ها را از  
سایت‌های رسمی دانلود کنید

۵ در هنگام عضویت از رمزهای  
عبور قوی استفاده کنید



## چگونه خریدی آنلاین و امن در فضای مجازی داشته باشیم؟

- ۱) نکات و توصیه‌های کاربردی برای انجام یک خرید اینترنتی ایمن بسیار ضروری است. قبل از خرید از فروشگاه اینترنتی، اعتبار آن فروشگاه را از طریق سایت نماد اعتماد الکترونیکی بررسی نمایید.
- ۲) ترجیحا از یک کارت بانکی مجزا با موجودی محدود برای خریدهای اینترنتی خود استفاده کنید تا در صورت افشای احتمالی اطلاعات کارت، امکان برداشت مبالغ هنگفت از حساب شما وجود نداشته باشد.
- ۳) در هنگام ثبت اطلاعات مالی و کارت بانکی خود حتما به آدرس درگاه پرداخت دقت داشته تا در دام صفحات جعلی و فیشینگ قرار نگیرید.
- ۴) در صورتی که قسط دارید یک اپلیکیشن فروشگاه اینترنتی را بر روی تلفن همراه خود نصب کنید
- ۵) در هنگام عضویت و استفاده از سایت از رمزهای عبور قوی و طولانی استفاده کنید که به سادگی قابل حدس زدن نیستند.

# مراقب کلاهبرداری

## با ترغیب هراچی های آنلاین باشید!



✕

فرب آههی های منتشر شده در کانال ها، صفحک و گروه های شبکه های اجتماعی با وعده های حراج آنلاین، تخفیفات ویژه و قیمت های باور نگرذنی را نخورید، پایین بودن بیس از حد قیمت می تواند ترغیبی برای ایجاد هیجان و عجله در خرید و کلاهبرداری از کاربران باشد.

▲ # خرید - امن



## حراجی های آنلاین و کلاهبرداری اینترنتی

مراقب کلاهبرداری با ترفند حراجی های آنلاین باشید! سوءاستفاده از مناسبت های مختلف یکی از مهمترین شگردهای مجرمان سایبری است. مناسبت های مذهبی، مناسبت های تفریحی، مناسبت های فصلی، بازگشایی مدارس، تعطیلات مختلف (نوروزی، تابستانی) و ... از جمله زمان هایی هستند که احتمال کلاهبرداری از هموطنان افزایش پیدا می کند.

یکی از مهمترین مناسبت هایی که احتمال افزایش جرائم سایبری را بالا می برد، فصل پاییز و حراجی های پاییزی هست. با توجه به بازگشایی مدارس و همچنین در پیش بودن فصل سرما، لذا خرید و فروش لباس های پاییزی و زمستانی مورد استقبال کاربران فضای مجازی قرار می گیرد. نکته مهم اینکه نقش تبلیغات در وقوع یک جرم سایبری بسیار پررنگ خواهد بود. بنابراین هموطنان گرامی نباید به فریب تبلیغات رنگارنگ و اغوا کننده را بخورند چرا که مجرمان سایبری با جلب اعتماد کاربران، به دنبال عملی کردن اهداف مجرمانه خود می باشند.

هموطنان گرامی این نکته را در نظر داشته باشید که تخفیفات ویژه و ارائه قیمت های بسیار پایین تنها برای ترغیب شما به خرید بوده و این احتمال وجود دارد تا با ایجاد هیجان و جو رقابتی بین کاربران، زمینه سرقت اطلاعات بانکی و در نهایت برداشت غیر مجاز از حساب های بانکی قربانیان را فراهم کنند. پس مراقب بوده و فریب پیچ ها و فروشگاه های غیر معتبر را نخورید.

#  
خرید امن

## آگهی های جعلی در کمین شهروندان



## ✗ روش کلاهبرداری

یکی از شگردهای مجرمان سایبری برای کلاهبرداری از شهروندان انتشار آگهی های جعلی به عنوان فروش محصولات ارزان قیمت در سایت های واسط فروشگاهی می باشد.

## ✓ راهکارهای پیشگیری

۱ به سادگی فریب وعده های پوچ و تبلیغات اغواکننده کلاهبرداران را نخورید.

۲ قبل از رویت و اطمینان از اصالت و مدارک کالا اقدام به پرداخت بیعانه نکنید.

۳ کاربران حتما در خصوص صحت هویت فرد آگهی دهنده بررسی های لازم را صورت دهند

۴ برای خرید حتما از فروشگاه هایی که دارای نماد اعتماد الکترونیکی هستند اقدام کنید.



## تبلیغات جذاب و البته جعلی در کمین کاربران فضای مجازی

یکی از شگردهای مجرمان سایبری برای کلاهبرداری از شهروندان انتشار آگهی‌های جعلی به عنوان فروش محصولات ارزان قیمت در سکوهای آگهی است. محصولاتی که وجود خارجی نداشته و تنها با هدف کلاهبرداری به فروش گذاشته شده‌اند. پس هموطنان گرامی باید ابتدا اصالت آگهی‌های درج شده و محصولات را بررسی و سپس اقدام به خرید و پرداخت وجه نمود.

مهمترین ترفندهای مجرمانه در فروش محصولات در سایت‌های واسطه:

- دریافت بیعانه و پیش پرداخت
- عدم ارسال کالا
- ارسال کالای فاقد کیفیت و کالای تقلبی و غیر مجاز
- نکات مهمی که کاربران باید رعایت کنند تا آگهی دهندگان جعلی را در رسیدن به اهدافشان ناکام گذاشت عبارتند از:
- عدم توجه به وعده‌های پوچ و تبلیغات اغواکننده در سایت‌های درج آگهی
- عدم پرداخت بیعانه و پیش پرداخت
- بررسی و احراز هویت فرد آگهی دهنده
- خرید کردن از سایت‌های فروشگاهی دارای نماد اعتماد الکترونیکی
- عدم توجه به لینک‌های اعلام شده در صفحات و پیج‌های فروشگاهی

# #خرید\_امن



**مراقب باشیم**

پلیس فضای تولید و تبادل اطلاعات ناجا

www.cyberpolice.ir



**شبکه های اجتماعی**

**بستر مناسبی برای**

**خرید اینترنتی نمی باشند**



## شبکه های اجتماعی بستری نا مطمئن برای انجام خرید های اینترنتی

خرید کردن در فضای مجازی از طرق مختلف انجام می شود که مهمترین ایمن ترین آنها خرید کردن از سایت های فروشگاههای دارای نماد اعتماد الکترونیک است. اما در فضای مجازی راه های دیگری نیز برای انجام خرید های اینترنتی وجود دارد که با مخاطرات زیادی همراه خواهند بود. یکی از این بستر ها، خرید کردن از صفحات فروشگاههای در پیام رسان ها و شبکه های اجتماعی است.

از آنجایی که فعالیت در شبکه های اجتماعی بدون احراز هویت صورت می گیرد لذا هر شخص با هر نام و عنوان و حتی با استفاده از شماره تلفن های فاقد سند می تواند اقدام به فعالیت نماید. پس لازم و ضروری است قبل از هرگونه خرید و تراکنش بانکی حتما نسبت به اصالت و اعتبار فروشگاه و فرد آگهی دهنده اطمینان پیدا شود.

نکته قابل تامل اینکه، شبکه های اجتماعی بستر مناسبی برای خرید اینترنتی نمی باشند. پس مراقب باشید تا فریب افراد سودجو را نخورید. این افراد با ایجاد پیج های فروشگاههای و ارائه محصولات مختلف و ارزان قیمت مشتری های خود را تشویق به انجام خرید اینترنتی کرده و در مرحله بعد اقدام به کلاهبرداری از وی می کنند.

نکته قابل توجه اینکه تعداد دنبال کننده زیاد دلیلی بر اصالت فروشگاه نیست چرا که امکان خرید دنبال کننده جعلی امکان پذیر است.

پس به صفحات فروشگاههای در شبکه های اجتماعی اطمینان نکنید.



# مراقب کلاهبرداری بباعنوان تخفیف‌های ویژه باشید

تخفیف ویژه‌ای برای شما در کار نیست

#خرید\_امن

پلیس فضای تولید و تبادل اطلاعات ناجا

www.cyberpolice.ir



## تخفیف های ویژه و باورنکردنی شگرد مجرمان سایبری



قیمت های باورنکردنی، تخفیف های ویژه، شارژهای ارزان قیمت و جملاتی از این قبیل ترافندی برای جذب مخاطب و دعوت از آنها برای بازدید و خرید محصولات می باشد. تبلیغاتی که روز به روز هدفمند و بیشتر شده است. برخی از این تبلیغات رنگ و بوی واقعیت نداشته و تنها برای جلب اعتماد کاربران و جذب مشتری بوده که در ادامه می تواند منجر به کلاهبرداری شود.

یکی از مهمترین روش های کلاهبرداری در این زمینه، راه اندازی حراجی های اینترنتی و جشنواره های مختلف فصلی است. در این مناسبت ها، تبلیغات گسترده ای صورت گرفته و با بهره بردن از شیوه های مختلف مهندسی اجتماعی سعی می کنند کاربران اینترنتی را ترغیب به خرید محصولات کنند.

عدم ارسال کالا، ارسال کالایی فاقد کیفیت لازم، دریافت بیعانه و پیش پرداخت از مهمترین روش های مجرمانه در این زمینه به شمار می رود که لازم است هموطنان گرامی در این خصوص دقت و توجه بیشتری داشته باشند.

مهمترین نکاتی که خریداران اینترنتی باید رعایت کنند عبارتند از:

- خرید از فروشگاه های معتبر و دارای نماد اعتماد الکترونیکی
- عدم پرداخت بیعانه و پیش پرداخت
- عدم توجه به تبلیغات جذاب و قیمت های پایین
- عدم خرید از پیج های فروشگاه های در شبکه های اجتماعی

هیچ‌ارزانی

بی‌علت

نیست



#کلیک\_امن

پلیس فضای تولید و تبادل اطلاعات ناجا

www.cyberpolice.ir



## هیچ ارزانی بی علت نیست. پس هوشیار باشید



وقتی به آگهی فروش اجناس با قیمت خیلی ارزان برخورد میکنید باید دقت و توجه بیشتری داشته و این ضرب المثل را به خاطر داشته باشید که «هرچه پول بدهی همان قدر آش می خوری» چون اجناس با کیفیت دارای قیمت هایی معقول می باشند. بنابراین هموطنان گرامی باید کمی با دید شک و تردید به موضوع ارزان بودن اجناس نگاه کنند.

معمولا ارزان بودن اجناس چند دلیل می تواند داشته باشد:

- کالای مورد نظر داری تخفیف ویژه می باشد.
- کالای مورد نظر دارای کیفیت لازم نیست.
- قیمت پایین برای جلب نظر کاربران ارائه شده و هدف آنان کلاهبرداری از کاربران هست.

بنابراین باید دقت و هوشیاری لازم را داشته باشیم.

برخی از افراد سود جو با ایجاد کانال و گروه های مختلف و صفحات تبلیغاتی با درج آگهی های جعلی و ارائه قیمت های بسیار پایین به دنبال هدایت کاربر به درگاه جعلی پرداخت (فیشینگ)، و در نهایت برداشت غیر مجاز از حساب بانکی آنها می باشند. بنابراین لازم است هموطنان گرامی قبل از هر گونه واریز وجه نسبت به اصالت فروشگاه اینترنتی و درگاه بانکی اطمینال حاصل کرده و فریب تبلیغات اغوا کننده را نخورند.

# کلاهبرداری اینستاگرامی در پوشش فروش کالا

کلاهبرداران با خرید پیج‌های اینستاگرامی با دنبال‌کننده (فالوئر) بالا و یا ساخت حساب کاربری با نام فروشگاه اقدام به فروش اجناسی می‌کنند که یا وجود خارجی ندارند یا تقلبی و با کیفیت بسیار پایین هستند.

## چگونه خرید امن داشته باشیم؟

کالا را به صورت پرداخت در محل سفارش داد و به هیچ عنوان قبل از دریافت و بررسی کالا مبلغ آن را برای فروشنده واریز نکنید.

بهتر است از پیج‌هایی خرید کنید که پشتوانه سایت دارای نماد اعتماد الکترونیک دارند و یا فروشگاه را در فضای حقیقی می‌شناسید.

در هنگام خرید مراقب لینک‌های جعلی ارسال شده توسط کلاهبرداران باشید و به هیچ عنوان روی آنها کلیک نکنید.



## # خرید امن

## کلاهبرداری اینستاگرامی در پوشش فروش کالا

کلاهبرداران با خریدن صفحات اینستاگرامی که دارای دنبال کننده های زیادی هستند سعی دارند فعالیت های اینترنتی خود را موجه جلوه داده و اقدام به فروش اجناس تقلبی و فاقد کیفیت کنند که یا وجود خارجی نداشته و یا سعی دارند کاربران را به لینک های جعلی (فیشینگ) هدایت کنند که در نهایت می تواند منجر به سرقت اطلاعات بانکی قربانیان شود.

در اینجا معمولا قربانیان فریب تعداد دنبال کننده بالا و تخفیف های ارائه شده را می خورند و به راحتی پرداخت وجه را انجام می دهند. در این بخش دو حالت می تواند رخ دهد:

1. هدایت به درگاه بانکی جعلی و سرقت اطلاعات بانکی.
  2. دریافت وجه توسط فروشنده و عدم ارسال کالا و یا ارسال کالای فاقد کیفیت
- بنابراین لازم است کاربران گرامی حساس تر بوده و با دقت بیشتری اصالت فروشگاه های اینترنتی و مجوزهای آنان را بررسی نمایند.
- توصیه پلیس فتا به شهروندان محترم، عدم خرید از صفحات فروشگاههای در شبکه های اجتماعی است. چراکه هیچ گونه تضمینی وجود ندارد که شما خریدی امن داشته باشید. این نکته را در نظر داشته باشید که تعداد دنبال کننده هیچ ملاکی برای مطمئن بودن بیج فروشگاههای نیست.



# از فروشگاه‌های اینترنتی مطمئن خرید کنید

در هنگام خرید اینترنتی، مراقب لینک‌های جعلی که  
کلاهبرداران برای شما ارسال می‌کنند باشید.

#خرید\_امن



هنگام خرید اینترنتی، از فروشگاه‌های مطمئن و دارای نماد اعتماد الکترونیک خرید کنید.

در زمان پرداخت وجه به نشانی درگاه پرداخت دقت کنید که حتما به دامنه [shaparak.ir](http://shaparak.ir) ختم شده باشد.



## فقط از فروشگاه‌های مطمئن و دارای مجوز خرید کنید

برخی از کلاهبرداران سایبری با بهره بردن از تبلیغات در کانال‌های تلگرام و استفاده از ربات‌های تلگرامی با ایجاد کانال‌های فروش انواع کالاها، کاربران را به صفحات درگاه‌های جعلی هدایت کرده و با شگرد فیشینگ، اقدام به اخذ مشخصات کارت بانکی، رمزهای عبور کرده و به دنبال خالی کردن حساب آن‌ها در فرصت مناسب هستند.

پلیس فتا با تأکید بر هوشیاری هموطنان چه در فضای حقیقی و چه در فضای مجازی از هموطنان در خواست دارد: با مطالعه و یادگیری در مورد نحوه خرید اینترنتی ایمن، نحوه پرداخت الکترونیکی در فضای مجازی و آشنایی با چگونگی تشخیص صفحات جعلی در دام کلاهبرداران نیفتند و در هنگام ثبت سفارشات اینترنتی از فروشگاه‌های دارای نماد اعتماد الکترونیک خرید و در زمان پرداخت وجه به نشانی درگاه پرداخت دقت کنند که حتما به دامنه [shaparak.ir/](http://shaparak.ir) ختم شده باشد.

همچنین کاربران گرامی باید این نکته را در نظر داشته باشند که خرید کردن از سایت‌های دارای نماد اعتماد الکترونیکی می‌تواند تا حد بسیار زیادی امنیت شما در خریدهای اینترنتی را افزایش دهد.

**سامانه پیامکی حساب‌های بانکی خود را همواره فعال  
کنند تا با دریافت پیامک از طرف بانک مربوطه از انجام  
عملیات بانکی مورد نظر اطمینان حاصل کنید.**



**#خرید\_امن**

پلیس فضای تولید و تبادل اطلاعات ناجا  
[www.cyberpolice.ir](http://www.cyberpolice.ir)



**مراقب باشیم**

## فعال کردن سامانه پیامکی راهکاری برای ارتقاء امنیت کاربران



برخی از مجرمان سایبری با بهره بردن از شیوه های مختلف مهندسی اجتماعی به دنبال کلاهبرداری از هموطنان هستند و این بار فروشندگان کالا در فضای مجازی مورد هدف آنان قرار گرفته اند. این افراد پرداخت وجه را در هنگام دریافت کالا انتخاب می کنند. شگرد مجرمانه این افراد بدین صورت است که بعد از انتخاب کالا و در هنگام پرداخت وجه مورد نظر اقدام به ارائه رسید بانکی جعلی، ارائه تصویر پرداخت و ... نموده و در قبال این مدارک خواستار دریافت کالای مورد نظر می باشند.

فروشندگان گرامی باید این نکته را در نظر داشته باشند که با استفاده از برنامه های رسید ساز جعلی می توان رسید های بانکی که بسیار شبیه به رسید های اصلی هستند، طراحی کرد. پس روئیت رسید بانکی نمی تواند به تنهایی مطمئن باشد. از جمله مواردی که می تواند امنیت خاطر لازم برای هموطنان عزیز را به دنبال داشته باشد، فعال سازی سامانه پیامکی حساب بانکی است که توسط سرشماره مشخص و منحصر به فرد بانک مربوطه برای کاربران ارسال می شود. در این حالت کاربران عزیز می توانند اطمینان داشته باشند که وجه مورد نظر به حساب بانکی آنان واریز شده است.



# عدم تامین کالا

در صدر شکایت خریداران اینترنتی

#خرید\_امن

پلیس فضای تولید و تبادل اطلاعات ناجا

www.cyberpolice.ir



## عدم ارسال کالا شگرد مجرمان سایبری

بررسی پرونده‌های تشکیل شده در پلیس فتا نشان می‌دهد عدم ارسال کالا به عنوان یکی از مهمترین شگردهای مجرمانه توسط سودجویان سایبری به شمار می‌رود که این موضوع شاکیان بسیاری داشته و علی‌رغم هدرهای داده شده و اطلاع‌رسانی‌های صورت گرفته متأسفانه همچنان شاهد وقوع اینگونه جرائم در بستر فضای مجازی و بخصوص شبکه‌های اجتماعی هستیم.

عدم پرداخت بیعانه و خرید کردن از سایت‌ها و فروشگاه‌های معتبر یکی از مهمترین راه‌کارهای مقابله با اینگونه جرائم محسوب می‌شوند.

بنابراین خرید از سایت‌های دارای نماد اعتماد الکترونیکی و همچنین خرید از صفحات پر مخاطب و معتبر می‌تواند اطمینان شما از داشتن خریدی ایمن را افزایش دهد.



# مراقب

## رسیدهای واریز جعلی

# باشید.

### #کلیک\_امن

استفاده از نرم افزارهای مختلف رسید ساز، شگرد این مجرمان برای کلاهبرداری از فروشندگان است. حتما پیامک بانکی خود را فعال کنید تا هرگونه واریز و برداشتی به آنها اطلاع داده شود تا به راحتی در دام مجرمان سایبری گرفتار نشوند، همچنین کلاههای ارسالی توسط پیک بعد از تأیید واریز از سوی آنها تحویل خریدار شود.

# مراقب باشیم

پلیس فضای تولید و تبادل اطلاعات ناجا  
www.cyberpolice.ir



## مراقب رسید سازهای واریز جعلی باشید



فروشنده‌گان عزیز مراقب باشید مورد سوء استفاده سودجویان سایبری قرار نگیرید. فروشنده‌گان اینترنتی ممکن است هدف کلاهبرداری مجرمان سایبری قرار بگیرند و با شیوه‌های مختلف از آنان کلاهبرداری شود. یکی از مهمترین شیوه‌های کلاهبرداری عدم واریز وجه به حساب آنان و دریافت کالا هست. روش کلاهبرداری به این صورت هست که بعد از دریافت کالا و در هنگام پرداخت وجه، یک سری مشخصات اولیه شامل نام و نام خانوادگی، شماره کارت بانکی مقصد و نام بانک مورد نظر از فروشنده دریافت شده و در ادامه با استفاده از برنامه‌های مجرمانه رسیدساز جعلی اقدام به طراحی رسید پرداخت وجه با نام فرد قربانی و بانک مورد نظر به همراه مبلغ، تاریخ و ساعت واریز نموده و در ادامه آن رسید را به رویت قربانی می‌رساند. در نگاه اول همه چیز عادی و درست به نظر می‌رسد. ظاهر رسید جعلی کاملاً شبیه به سایر رسیدهای پرداخت بوده و هیچ‌گونه تفاوتی وجود ندارد. تنها تفاوت این رسیدسازهای جعلی عدم واریز وجه به حساب فرد قربانی است که معمولاً با تراکنش‌های بالای بانکی و ... توجیه خواهد شد.

هموطنان گرامی در نظر داشته‌باشند اطمینان از واریز وجه از طریق پیامک و یا اینترنت بانک می‌تواند اطمینان خاطر را برای آنان به همراه داشته‌باشد.



# نکات کلیدی خرید امن آنلاین



با توجه به دامن‌گیر شدن کرونا در کشور، اغلب کسب و کارها به راه‌اندازی فروشگاه‌های مجازی روی آورده‌اند. در این میان افراد سودجو همواره از فرصت‌ها استفاده نموده و با ایجاد فروشگاه‌های جعلی اقدام به کلاهبرداری‌های مالی از قربانیان می‌نمایند. کاربران به هنگام خریدهای اینترنتی هوشیار بوده تا در دام افراد سودجو قرار نگیرند.

## برای جلوگیری از سوءاستفاده مجرمین



با توجه به افزایش کانال‌ها و صفحات فروش کالا و خدمات در شبکه‌های اجتماعی کاربران فریب تبلیغات و تخفیفات ویژه این صفحات را نخورده و مراقب باشند در دام کلاهبرداران سایبری گرفتار نشوند. شهروندان کالا و اقلام موردنیاز خود را از سایت‌های فروشگاه‌های معتبر که دارای نماد الکترونیکی هستند تهیه نمایند.

قبل از هرگونه معامله‌ای، ابتدا آدرس و شماره تلفن فروشنده را بررسی و نسبت به صحت آن اطمینان حاصل نمایید.

قبل از رویت و تحویل کالا هیچ‌گونه مبلغی تحت عنوان بیعانه به حساب فروشنده واریز ننمایید.

## نکات کلیدی در خرید امن آنلاین



کاربران به هنگام خریدهای اینترنتی هوشیار بوده تا در دام افراد سودجو قرار نگیرند. پس این نکات را در نظر داشته باشید:

۱- با توجه به افزایش کانال‌ها و صفحات فروش کالا و خدمات در شبکه‌های اجتماعی، فریب تبلیغات و تخفیفات ویژه این صفحات را نخورده و مراقب باشید در دام کلاهبرداران سایبری گرفتار نشوید.

۲- شهروندان، کالا و اقلام موردنیاز خود را از سایت‌های فروشگاهی معتبر که دارای نماد الکترونیکی هستند تهیه نمایند.

۳- قبل از هرگونه معامله، ابتدا آدرس و شماره تلفن فروشنده را بررسی و نسبت به صحت آن اطمینان حاصل نمایید.

۴- قبل از رویت و تحویل کالا هیچ‌گونه مبلغی تحت عنوان بیعانه به حساب فروشنده واریز ننمایید.

#خرید\_امن

## شگرد کلاهبرداران در سایت های درج آگهی

انتشار آگهی، جلب اعتماد  
مشتری و دریافت بیعانه

در این صورت یا کالایی برای مشتری  
ارسال نخواهد شد و یا کالای ارسالی  
فاقد کیفیت لازم است



## کلاهبرداری در سایت های درج آگهی



ثبت و انتشار آگهی، استفاده از جملات جذاب و اغوا کننده، ارائه قیمت هایی کمتر از عرف بازار، دریافت بیعانه، عدم ارسال کالا، ارسال کالای تقلبی و .... روندی است که یک فرد مجرم برای کلاهبرداری از کاربران فضای مجازی طی می کند. مهمترین نکته در رسیدن مجرم سایبری به اهدافشان، اعتماد خریداران به تبلیغات انجام شده و همچنین عدم توجه قربانیان به نکات ایمنی در فضای مجازی هست. بنابراین هموطنان عزیز:

- فریب تبلیغات اغوا کننده را نخورید
- از پرداخت هرگونه وجه تا قبل از دریافت کالا امتناع کنید در غیر این صورت یا کالایی برای شما ارسال نخواهد شد و یا کالای ارسالی فاقد کیفیت لازم است .
- به لینک های ارائه شده در پیام ها و تبلیغات اعتنا نکنید.
- با فعال سازی سامانه پیامکی حساب بانکی از تراکنش های خود مطلع شوید.



پلیس فضای تولید و تبادل اطلاعات

# دریافت بیعانه

## شگردی که کهنه نمی شود

هرگونه پرداخت بیعانه در فروشگاه های آنلاین می تواند زمینه ساز کلاهبرداری اینترنتی از کاربران گردد.

### برای جلوگیری از سوءاستفاده مجرمین

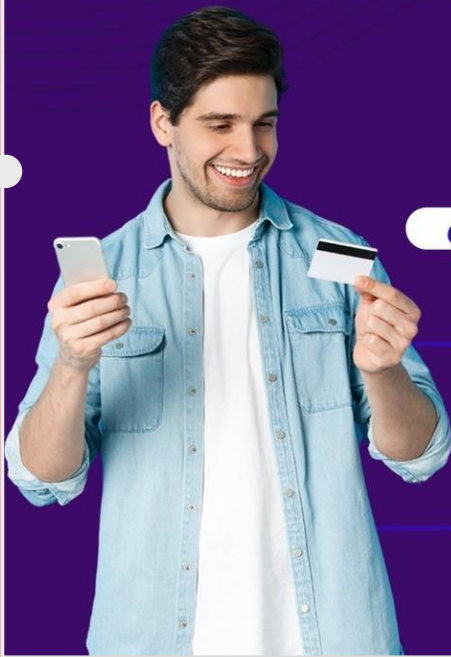


۱ تحت هیچ عنوان پیش از رویت و دریافت کالا مبلغی تحت عنوان بیعانه پرداخت نکنید.

۲ بعد از دریافت کالا و اطمینان از صحت و اصالت کالا اقدام به پرداخت وجه نمایید.

۳ برای خرید امن حتما از فروشگاه های معتبر و دارای نماد اعتماد الکترونیکی اقدام به خرید نمایید.

۴ خرید از فروشگاه هایی که در شبکه های اجتماعی فعالیت دارند می تواند زمینه ساز کلاهبرداری اینترنتی گردد.



# خرید امن

CYBERPOLICE.IR

دانشتهای سایبری

www.cyberpolice.ir

۷۲

## دریافت بیعانه شگردی قدیمی اما رایج

دریافت بیعانه، شگردی که کهنه نشده و همچنان قربانی می‌گیرد. بر اساس پرونده‌های متشکله در پلیس فتا، دریافت بیعانه همچنان به عنوان یکی از مهمترین شگردهای مجرمانه در حوزه کلاهبرداری‌های مالی به شمار می‌رود و آمار بالای مال باختگان گواهی بر این موضوع خواهد بود. افراد سودجو با بهره‌بردن از شیوه‌های مختلف مهندسی اجتماعی، چرب‌زبانی، ارائه اجناس با کیفیت ولی با قیمت‌های پایین و ... سعی در جلب اعتماد قربانیان داشته و در ادامه از آنان کلاهبرداری خواهند کرد. دریافت بیعانه و عدم ارسال کالا از مهمترین شگردهای آنان به شمار می‌رود. پس هرگونه پرداخت بیعانه در فروشگاه‌های آنلاین می‌تواند زمینه‌ساز کلاهبرداری اینترنتی از کاربران گردد.

بنابراین برای جلوگیری از سوء استفاده مجرمین:

۱- تحت هیچ عنوان پیش از رویت و دریافت کالا مبلغی تحت عنوان بیعانه پرداخت نکنید.

۲- بعد از دریافت کالا و اطمینان از صحت و اصالت کالا اقدام به پرداخت وجه نمایید.  
 ۳- برای خرید امن حتماً از فروشگاه‌های معتبر و دارای نماد اعتماد الکترونیکی اقدام به خرید نمایید.

۴- خرید از فروشگاه‌هایی که در شبکه‌های اجتماعی فعالیت دارند می‌تواند زمینه‌ساز کلاهبرداری اینترنتی گردد.



# خرید امن

# رسیدهای جعلی شگردی برای کلاهبرداری از فروشندگان



یکی از شگردهای کلاهبرداران سایبری جهت سرقت اطلاعات کاربران طراحی ساخت اپلیکیشن رسیدساز جعلی می باشد. مجرمان با قرار دادن اطلاعات بانکی در برنامه رسیدساز فیش پرداختی شبیه فیش برنامه های پرداخت تهیه و به فروشندگان عرضه می کنند.

شهروندان حتما سامانه پیامکی حساب های بانکی خود را فعال نمایند تا با دریافت پیامک از طرف بانک از انجام هرگونه تراکنش بانکی مورد نظر اطمینان حاصل نمایند.

در صورت دریافت پیامک انتقال وجه حتما سر شماره آن را بررسی و با پیامک های قبلی خود تطبیق دهید و ارسال پیامک از سرشماره جدید را به عنوان سند قبول نکنید.

## رسیدهای جعلی شگردی برای کلاهبرداری از فروشندگان!

یکی از شگردهای کلاهبرداران سایبری جهت سرقت اطلاعات کاربران طراحی ساخت اپلیکیشن رسیدساز جعلی می باشد. مجرمان با ثبت اطلاعات بانکی در برنامه رسیدساز، اقدام به طراحی فیش پرداختی که از نظر ظاهری شبیه به فیش پرداخت اصلی است نموده و به فروشندگان ارائه می کنند.

از جمله اقداماتی که در صورت انجام می تواند تا حد بسیار زیادی مجرمان سایبری را در رسیدن به اهدافشان ناکام بگذارند عبارتند از:

- فعال کردن سامانه پیامکی: شهروندان حتما سامانه پیامکی حساب های بانکی خود را فعال نمایند تا با دریافت پیامک از طرف بانک از انجام هرگونه تراکنش بانکی مورد نظر اطمینان حاصل نمایند.
- دقت در سر شماره های بانکی: در صورت فعال بودن سامانه پیامکی به سرشماره ارسال کننده پیامک توجه داشته باشید و مطمئن شوید پیامک دریافتی از جانب بانک باشد.
- اینترنت بانک: مراجعه به اینترنت بانک و بررسی تراکنش های بانکی می تواند راه کار مناسبی برای ناکام گذاشتن مجرمان باشد.

# خرید امن

# کلاهبرداری اینترنتی در سایت های درج آگهی



آگهی های کلاهبردارانه چه نشانه هایی دارند:

این آگهی ها؛ قیمت های وسوسه انگیز و زیر قیمت بازار دارند

شماره تراکب می کنند تا قبل از رویت کالا مبلغی را پرداخت کنند

فروشنده از چندین نفر به صورت همزمان تقاضای بیعانه می کند



## کلاهبرداری های اینترنتی از طریق سایت های درج آگهی

سوء استفاده از آگهی های درج شده در سایت های درج آگهی رو به افزایش بوده و به یکی از مهمترین ترفند های مجرمان سایبری برای کلاهبرداری از هموطنان تبدیل شده است. ترفندی که متأسفانه زمینه ساز تشکیل پرونده های بسیار در پلیس شده و افراد سودجو با بهره بردن از شیوه های مهندسی اجتماعی و بعد از جلب اعتماد قربانیان توانسته اند مبالغ بالایی کلاهبرداری نمایند.

سوال مهمی که اینجا مطرح می شود این است که ، آگهی های جعلی را از واقعی چگونه تشخیص بدهیم و یا از کجا بدانیم که این آگهی جعلی است و برای کلاهبرداری طراحی شده یا خیر؟

در پاسخ باید گفت آگهی های جعلی چند ویژگی دارند که عبارتند از:

- قیمت های پایین، این آگهی ها معمولاً قیمت هایی پایین تر از عرف بازار داشته و به نوعی کاربران را تشویق به انجام ادامه کار می کنند.
  - دریافت بیعانه، این آگهی ها معمولاً قیمت های وسوسه انگیز و زیرقیمت بازار دارند و فروشنده شما را ترغیب می کند قبل از رویت کالا و برای جلوگیری از فروش آن به فرد دیگری، مبلغی را به عنوان بیعانه پرداخت کنید.
- بنابراین به شهروندان گرامی توصیه می شود فریب قیمت های پایین را نخورده و قبل از مراجعه حضوری به فروشنده مبلغی را تحت عنوان بیعانه پرداخت نکنند.

# خرید اینترنتی امن



## خرید اینترنتی ایمن چه ویژگی هایی دارد؟



کاربرانی که قصد خرید اینترنتی دارند جهت انجام یک خرید مطمئن، حتماً به نکات ذیل توجه نمایند:

- از هر فروشگاهی خرید نکنید: از فروشگاه‌هایی خرید خود را انجام دهید که دارای «نماد اعتماد الکترونیکی» باشد.
- از هر کامپیوتری برای خرید الکترونیکی استفاده نکنید: از خرید کردن با تجهیزات دیجیتالی دیگران یا مستقر در اماکن عمومی مانند نت‌سراها خودداری کنید.
- مراقب آدرس درگاه بانکی باشید: تمامی درگاه‌های بانکی به دامنه [shaparak.ir/](http://shaparak.ir) ختم می‌شوند پس، از اتصال به درگاه بانکی اصلی و سیستم بانک مرکزی مطمئن شوید.
- اطلاعات شخصی را در سایت‌ها ثبت نکنید: اطلاعاتی از جمله رمز دوم کارت، CVV2 و تاریخ انقضا را نباید در هیچ سایتی ذخیره کنید.
- بیعانه پرداخت نکنید: برخی از کلاه‌برداران با فریب خریداران به‌روش‌های مختلف از آنان بیعانه یا پیش‌پرداخت اخذ نموده و سپس از ارسال کالا خودداری می‌نمایند.
- از صفحات و کانال و گروه‌های موجود در شبکه‌های اجتماعی خرید نکنید: دقت کنید که اکثر این صفحات با درج پست‌های جعلی (فیش‌های بانکی، چت‌های رضایت مشتری و ...) قصد فریب کاربران را دارند.

# خرید امن

دانشی‌های سایبری

# پیشگیری از کلاهبرداری اینترنتی در پیامک رمز دوم پویا



جهت پیشگیری از کلاهبرداری اینترنتی  
در پیامک رمز دوم پویا  
به علت تراکنش و مبلغ آن توجه کنید.

www.cyberpolice.ir



cyberpolice.ir

پلیس فضای تولید و تبادل اطلاعات ناجا

## رمز دوم پویا راهکاری برای جلوگیری از برداشت غیر مجاز



رمز پویا توانسته تا درصد زیادی برداشت غیرمجاز را کاهش دهد و مجرمان را ناکام بگذارد ولی مجرمان حرفه ای با روش های پیچیده تر سعی دارند اعمال مجرمانه خود را ادامه دهند که استفاده از بدافزار های موبایلی از این روش هاست.

در این روش مجرمان سایبری با استفاده از مهندسی اجتماعی مانند ارسال پیامک های جعلی تحت عنوان سامانه ابلاغ اوراق قضایی (ثنا) ، کاربر را از طریق یک آدرس اینترنتی به صفحه ای جعلی هدایت می کنند و او را ترغیب به نصب برنامه موبایلی می کنند.

این برنامه موبایلی با ایجاد دسترسی غیرمجاز امکان سرقت پیامک رمزپویا را به مجرم می دهد.



## دانستنی‌های سایبری

این مجموعه به همت مرکز تشخیص و پیشگیری از جرایم سایبری پلیس فضای تولید و تبادل اطلاعات فراجا تهیه شده است، مجموعه‌ای از هشدارهای پیشگیرانه سایبری در موضوعات کلاهبرداری اینترنتی، حریم خصوصی و راه کارهای ارتقاء امنیت کاربری است.

