



هشدار:

مراقب کلاهبرداری در بازار رمزارزها باشید!



1 فریب وعده‌های «سودهای نجومی و تضمینی» در بازار رمزارزها را نخورید.



2 کلیدهای خصوصی (Private Keys) و عبارات بازیابی کیف پول خود را هرگز در اختیار کسی قرار ندهید.



3 برای خرید و فروش رمزارز، فقط از صرافی‌های معتبر و دارای مجوز قانونی استفاده کنید.



4 مراقب کانال‌ها و گروه‌های تلگرامی که وعده «سیگنال خرید یا فروش» می‌دهند باشید.



5 در صورت مواجهه با سایت‌های مشکوک یا کلاهبرداری، سریعاً به پلیس فتا گزارش دهید.



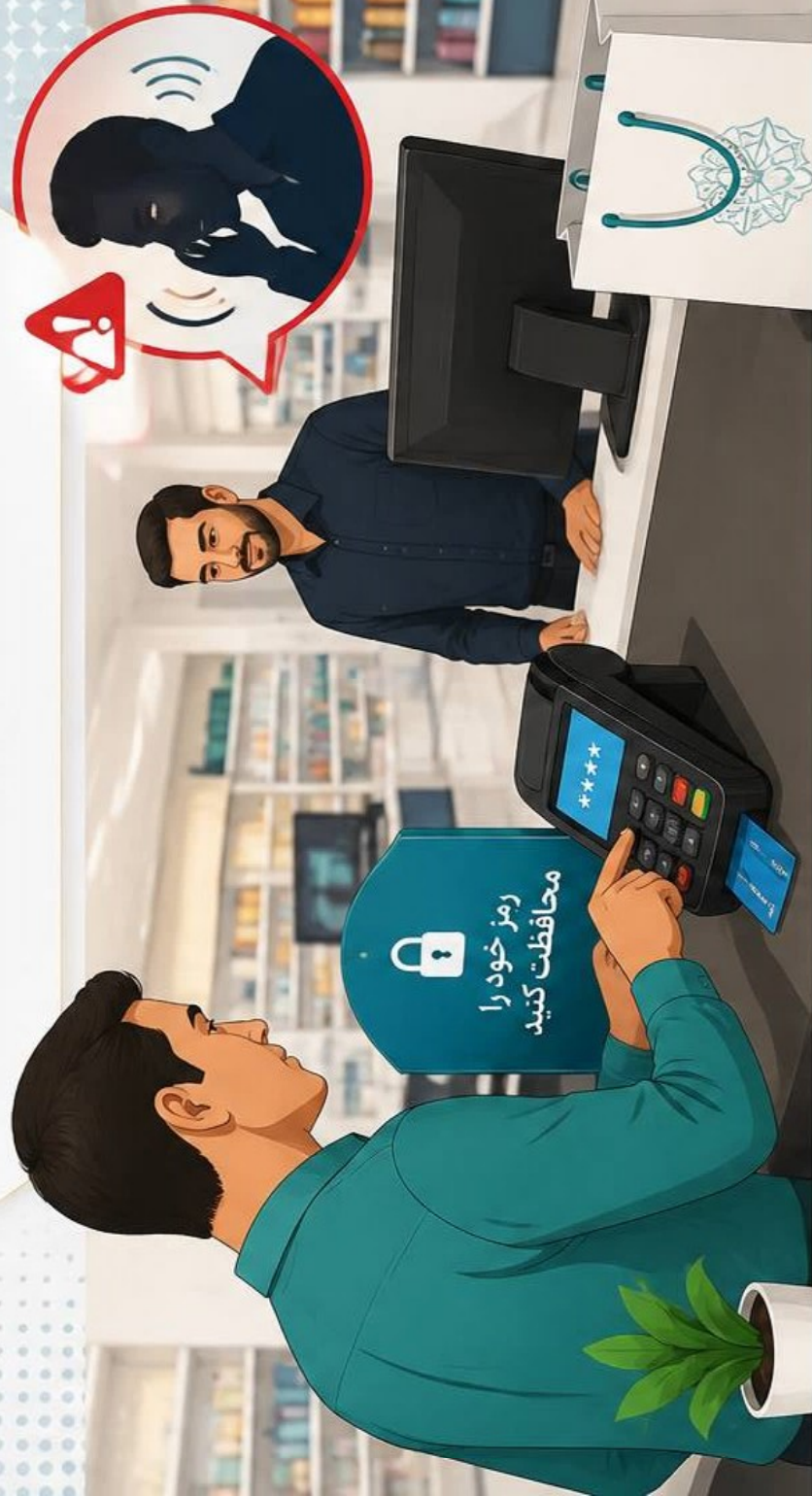
۰۹۶۳۸۰

www.cyberpolice.ir





اعلام بلند رمز کارت در فروشگاهها، نقض امنیت شماست؛ از این رفتار پرخطر پرهیز کنید



رمز کارت خود
را محرمانه نگه دارید



رمز خود را
بلند اعلام نکنید



در وارد کردن رمز،
مراقب اطراف باشید



حفاظت از اطلاعات بانکی،
حفاظت از دارایی شماست





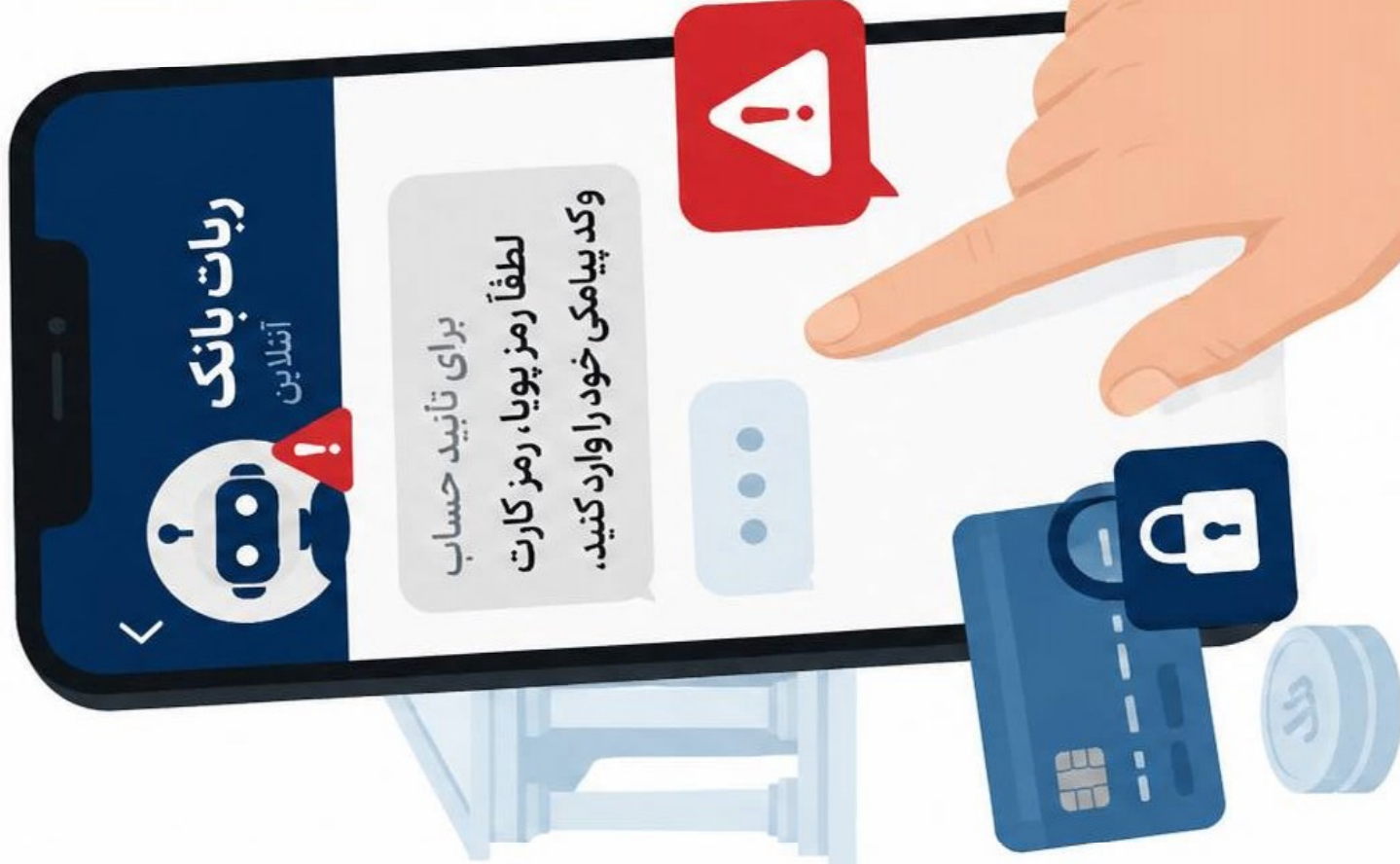
با جرایم فضای مجازی

ساخت حساب کاربری
با نام و تصویر دیگران،
مصدق **جعل رایانه‌ای**
و جرم دارای مجازات است



ربات جعلی بانک‌ها

به ربات‌های ناشناس اعتماد نکنید



برای تأیید حساب
لطفاً رمز پویا، رمز کارت
و کد پیامکی خود را وارد کنید.



بانک‌ها از شما
رمز پویا، رمز کارت
و کد پیامکی را
نمی‌خواهند



فقط از همراه بانک
و درگاه‌های رسمی
استفاده کنید



در صورت مشکوک شدن،
ارتباط را قطع و
موضوع را
گزارش کنید



هشدار امنیتی:

از نصب برنامه‌های مشکوک خودداری کنید.



۱



هرگز برنامه‌های کاربردی را از منابع غیررسمی (مانند لینک‌های ارسالی در تلگرام، واتس‌اپ یا پیامک‌های ناشناس) دانلود نکنید.

۲



نصب برنامه‌های ناشناس می‌تواند منجر به سرقت اطلاعات شخصی، دسترسی به مخاطبین و خالی شدن حساب بانکی شما شود.

۳



فقط از فروشگاه‌های رسمی معتبر (مانند کافه‌بازار یا گوگل‌پلی) استفاده کنید.

۴



به دسترسی‌های درخواستی برنامه هنگام نصب (دسترسی به پیامک‌ها و مخاطبین) حساس باشید.

پیام‌ها و تماس‌های «شما برنده شده‌اید» ترفند کلاهبرداران برای ترغیب به انتقال وجه است؛ فریب نخورید.



به پیام‌ها و تماس‌های
مشکوک پاسخ ندهید.



روی لینک‌های ناشناس
کلیک نکنید.



اطلاعات کارت بانکی
و رمز خود را وارد نکنید.



موارد مشکوک را به پلیس
فتا نیا شماره 110 گزارش دهید.



معاونت اجتماع، و پیشگیری، از وقوع جرم



هشدار:



مراقب کلاهبرداری

با عنوان فروش امتیاز وام و خودرو باشید!



به آگهی‌های فروش «امتیاز وام مسکن» یا «امتیاز خودرو» در فضای مجازی **اعتماد نکنید.**



انتقال امتیاز یک فرایند قانونی است که صرفاً باید از طریق بانک‌ها و نمایندگی‌های **رسمی** انجام شود.



از پرداخت هرگونه بیعانه یا مبلغی به عنوان «پیش‌پرداخت» یا «رزرو امتیاز» به افراد ناشناس اکیداً **خودداری کنید.**



بسیاری از این آگهی‌ها صرفاً برای **سرقت اطلاعات یا کلاهبرداری مالی** طراحی شده‌اند.



در صورت مشاهده موارد مشکوک، موضوع را سریعاً به **پلیس فتا** گزارش دهید.



امنیت شما، مسئولیت ماست.
با آگاهی، از خود و دیگران محافظت کنیم.



گزارش جرایم سایبری
به پلیس فتا
۰۹۶۳۸۰



هنگام خرید، کارت بانکی را
شخصاً در دستگاه کارتخوان بکشید
و رمز را خودتان وارد نمایید.



وام فوری
بدون ضامن!



کلاهبرداری

مراقب کلاهبرداری با عنوان وام فوری باشید!

هشدار:

دریافت وام



1 به وعده‌های «وام فوری» و «وام بدون ضامن»
در شبکه‌های اجتماعی اعتماد نکنید.



2 هیچ‌گونه وجهی را تحت عنوان «هزینه ثبت‌نام»
با «بیمه» قبل از دریافت وام پرداخت نکنید.



3 فرایند دریافت وام فقط از طریق شعب رسمی
بانک‌ها و سامانه‌های معتبر انجام می‌شود.



4 اطلاعات کارت بانکی و کدهای امنیتی
(رمز پویا) خود را هرگز در اختیار افراد
ناشناس قرار ندهید.



5 در صورت مشاهده پیشنهاد‌های مشکوک،
موضوع را سریعاً به پلیس فتا گزارش دهید.

از طریق هوش مصنوعی

کلاهبرداران با استفاده از هوش مصنوعی، صدای اقار را تقلید می‌کنند تا با جلب اعتماد شما، از نزدیکان یا سازمان‌ها پول یا اطلاعات حساس دریافت کنند.



ضبط صدا



پردازش با هوش
مصنوعی مصنوعی



تقلید صدا و
جلب اعتماد

کلاهبرداران می‌توانند با صدای تقلید شده از شما بخواهند پول واریز کنید یا اطلاعات محرمانه در اختیارشان قرار دهید.



راهکارهای پیشگیری



برای درخواست‌های مالی یا حساس، از روش دیگری (تماس تصویری یا مراجعه حضوری) اطمینان حاصل کنید.



اطلاعات شخصی، بانکی و رمزهای یکپار مصرف را هرگز در تماس تلفنی در اختیار کسی قرار ندهید.



در صورت شک و تردید، با نزدیکان خود مستقیماً تماس بگیرید و صحت موضوع را بررسی کنید.



به اه‌اطرافیان خود درباره روش‌های جدید کلاهبرداری با هوش مصنوعی آگاهی دهید.



هرگونه مورد مشکوک را فوراً به پلیس فتا (3838) گزارش دهید.

هوش مصنوعی

فریب نخورید



راهکارهای پیشگیری



هویت تماس گیرنده را به روش دیگر تأیید کنید.



اطلاعات شخصی و مالی خود را در تماس تلفنی ارائه ندهید.



به درخواست‌های عجولانه یا تهدیدآمیز مشکوک باشید.



از اجرای لینک‌ها و نصب برنامه‌های ناشناس خودداری کنید.



موارد مشکوک را به پلیس فتا یا مراجع قضایی گزارش دهید.



هوش مصنوعی می‌تواند صدا را تقلید کند؛
هوشیار باشید و امنیت خود و دیگران را حفظ کنید.



نشانه‌های هشدار



صدای غیرطبیعی
با بیش از حد
کامل و بدون نقص



ایجاد حس فوریت و
فشار برای تصمیم‌گیری
سریع



درخواست اطلاعات
حساس مانند رمزها،
کدها و حساب بانکی



ادعای واریز جایزه، بدهی،
مشکله امنیتی یا مسائل
قضایی



استفاده از صداهای
شبه‌سازی شده نزدیکان
یا مدیران

پیشگیری از جرایم فضای مجازی



طبق قانون جرایم رایانه‌ای،
انتشار تصاویر، ویدیوها یا
اسرار خصوصی دیگران
در فضای مجازی، مجازات
حبس و جزای نقدی دارد.





هشدار: مراقب اسکیمرها باشید!

نکات مهم برای پیشگیری از کلاهبرداری در دستگاه‌های کارت‌خوان

۱

کارت بانکی خود را به فروشنده ندهید؛
شخصاً رمز عبور را وارد کنید.



۲

از پوشاندن دست هنگام وارد کردن
رمز عبور غافل نشوید.



۳

در صورت مشاهده **قطعه اضافی** یا
مشکوک روی دستگاه کارت‌خوان،
از خرید **منصرف شوید**.



۴

رمز کارت بانکی خود را به صورت
دوره‌ای **تغییر دهید**.



۵

پیامک‌های بانکی خود را فعال و
تراکنش‌های حساب را مرتب چک کنید.





هشدار:

مراقب کلاهبرداری اینترنتی باشید



اطلاعات کارت بانکی، رمز پویا و
کدهای پیامکی را در اختیار
هیچ کس قرار ندهید.



پیش از پرداخت، نشانی
اینترنتی، اعتبار فروشگاه و
درگاه پرداخت را بررسی کنید.



برای دریافت جایزه، وام یا
خدمات قوری، روی لینک‌های
ناشناس کلیک نکنید.



برای انتقال وجه، از احراز هویت
و بررسی نام صاحب حساب
اطمینان حاصل کنید.



در صورت وقوع جرم، مستندات را حفظ و موضوع را
سریعاً به پلیس فتا و مراجع قانونی گزارش کنید.



هیچ سازمان معتبری رمز کارت با کد تأیید پیامکی شما را درخواست نمی‌کند.





با جرایم فضای مجازی

هنگام خرید از دیوار، شیپور، ترب و سایر سکوهاى خرید و فروش:



۱

بررسی هویت فروشنده
و اصالت کالا قبل از پرداخت



۲

خودداری از پرداخت پيغامانه
به حساب‌های ناشناس



۳

استفاده از درگاه‌های
پرداخت امن و رسمی



۴

عدم کلیک بر روی
لینک‌های ناشناس و مشکوک



۵

گزارش سریع موارد مشکوک
به پلیس فتا



خرید امن، با آگاهی و احتیاط
امنیت شما، مسئولیت شماست

دوستان و نزدیکان؟

ممکن است کلاهبرداری سایبری باشد!



فوری پول واریز نکنید!



تعمیل نکنید



شماره کارت
نفرستید



روی لینک‌های
مشکوک کلیک نکنید

ابتدا بررسی و
اطمینان حاصل کنید



تماس بگیرید و
مستقیم گفتگو کنید



هویت درخواست‌کننده
را مطمئن شوید



هوشیار باشید
امنیت، مسئولیت همه‌ماست



کلاهبرداران سایبری با دستکاری حساب‌های کاربری افراد،
از نام و اعتبار آن‌ها برای **فرب** شما استفاده می‌کنند.

معاونت اجتماعی و پیشگیری از وقوع جرم





هشدار:

پیامک‌های جعلی ابلاغ الکترونیک قضایی



۱

پیامک واقعی ابلاغیه
فقط با سرشماره
ADLIRAN ارسال می‌شود
و شماره شخصی نیست.



۲

ابلاغیه قضایی هرگز
حاوی لینک پرداخت وجه
یا دانلود فایل/برنامه
(APK) نمی‌باشد.



۳

ورود به سامانه ثنا
صرفاً از نشانی رسمی
امکان پذیرت. **adliran.ir** است.



به لینک‌های مشکوک در پیامک‌ها، شبکه‌های اجتماعی و ایمیل‌ها
اعتماد نکنید و از وارد کردن اطلاعات شخصی خودخوداری نمایید.



پرسشگیری و مقایسه با جرایم فضای مجازی

مسئله
آرم پیشگیری
از وقوع جرم

هنگام خرید از دیوار، شیپور، ترب و سایر سکوهای خرید و فروش:



خرید امن، با آگاهی و احتیاط
امنیت شما، مسئولیت شماست



سود تضمینی
بازدهی نجومی
درآمد بالا

هشدار مهم



وعده‌های نجومی و تضمینی

در فضای مجازی و
بازار ارز دیجیتال،
دامی برای غارت
سرمایه شماست



سودهای غیرواقعی
وجود ندارد



پلتفرم‌های ناشناس و
بدون مجوز، خطرناک‌اند



اطلاعات شخصی و مالی خود
را در اختیار دیگران قرار ندهید



قبل از سرمایه‌گذاری،
تحقیق و بررسی کنید

پیش از هر پرداخت، از صحت آدرس
و نماد اعتماد الکترونیکی و **shaparak.ir**
(اینماد) اطمینان حاصل کنید



نماد اعتماد الکترونیکی
(اینماد)

www.enamad.ir

✓ سایت مورد تأیید و معتبر است



استفاده از درگاه پرداخت معتبر (shaparak.ir)



بررسی نماد اعتماد الکترونیکی (اینماد)



عدم ورود اطلاعات کارت در سایت‌های نامعتبر



اطلاعات کارت خود را
در اختیار دیگران قرار
ندهید



همواره آدرس سایت
را در مرورگر بررسی
کنید



به پیامک‌ها و لینک‌های
مشکوک پاسخ
ندهید



از آنتی‌ویروس به‌روز
و فایروال استفاده
کنید

