بسم الله الرحمن الرحیم

امن سازی پیامرسان های موبایلی

ضرورت توجه به امن سازی پیام رسان ها و راهکارهای
امن سازی پیام رسان های ایرانی

انتشار تصاویر خصوصی در فضای مجازی

آشنایی با خطرات و راهکارهای پیشگیری از انتشار
تصاویر خصوصی در فضای مجازی

بسم الله الرحمن الرحیم

کلاهبرداری در بسترسایت های ثبت آگهی

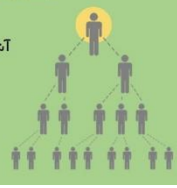
آشنایی با راهکارهای پیشگیری از کلاهبرداری در بستر سایت
های ثبت آگهی در فضای مجازی

کلاهبرداری پیامکی

آشنایی با شگردهای کلاهبرداری از طریق ارسال پیامک
های جعلی در فضای مجازی

کلاهبرداری جذب سرمایه

آشنایی با شگردهای کلاهبرداری از طریق جذب سرمایه در
فضای مجازی



حریم خصوصی چیست؟

به مجموعه حقوق و آزادی‌هایی اطلاق می‌شود که فرد برای **حفظ داده‌ها، اطلاعات، فعالیت‌ها و هویت شخصی** خود در فضای مجازی دارد.

حریم خصوصی در فضای مجازی شامل چه موضوعاتی می‌شود

۱. اطلاعات شخصی	•نام، آدرس، شماره تلفن، ایمیل، اطلاعات شناسنامه
۲. تاریخچه فعالیت‌ها	•تاریخچه فعالیت‌های برخط کاربر در فضای مجازی مانند خرید و جستجوها
۳. مکان	•اطلاعات مربوط به محل و موقعیت جغرافیایی
۴. فعالیت‌های آنلاین	•مرور صفحات وب، استفاده از نرم‌افزارها، ارسال و دریافت پیام، مشارکت در شبکه‌های اجتماعی
۵. اطلاعات مالی	•شامل شماره کارت اعتباری، اطلاعات بانکی و سایر اطلاعات مربوط به معاملات مالی
۶. ارتباطات	•ایمیل، پیام‌رسان‌ها، تماس‌ها، نظرات، شبکه دوستان و پیام‌های خصوصی
۷. اطلاعات پزشکی	•اطلاعات مربوط به سابقه بیماری‌ها، نتایج آزمایش‌ها و سایر اطلاعات درمانی
۸. حریم فردی	•تصاویر شخصی، شامل عکس‌ها، ویدئوها و سایر محتواهای شخصی کاربر

انواع کاربران از نظر سطح توجه به حریم خصوصی

کاربران خصوصی (Privacy Fundamentalists)

- این افراد به شدت حساس هستند و بسیار نگران حفظ حریم خصوصی خود در فضای مجازی هستند. آن‌ها به ندرت اطلاعات شخصی خود را در اینترنت به اشتراک می‌گذارند و معمولاً مخالف استفاده از اطلاعات شخصی خود برای هر گونه منظور تجاری یا بازاریابی هستند

کاربران واکنش‌گر (Privacy Pragmatists)

- این دسته از کاربران واکنش‌های متوازن‌تری نسبت به حفظ حریم خصوصی دارند. آن‌ها ممکن است اطلاعات شخصی خود را به اشتراک بگذارند اگر فکر کنند که از آن استفاده کردن به آن‌ها منافعی دارد، و همچنین به شرکت‌ها اعتماد دارند که اطلاعاتشان را به درستی محافظت کنند

کاربران بی‌توجه (Privacy Unconcerned)

- این افراد آگاهی یا نگرانی چندانی نسبت به مسائل حفظ حریم خصوصی ندارند. آن‌ها فکر نمی‌کنند که نقض حریم خصوصی ممکن است برای آن‌ها مشکلی ایجاد کند و معمولاً بدون تامل به اشتراک‌گذاری اطلاعات پرداخته و از خدمات آنلاین استفاده می‌کنند

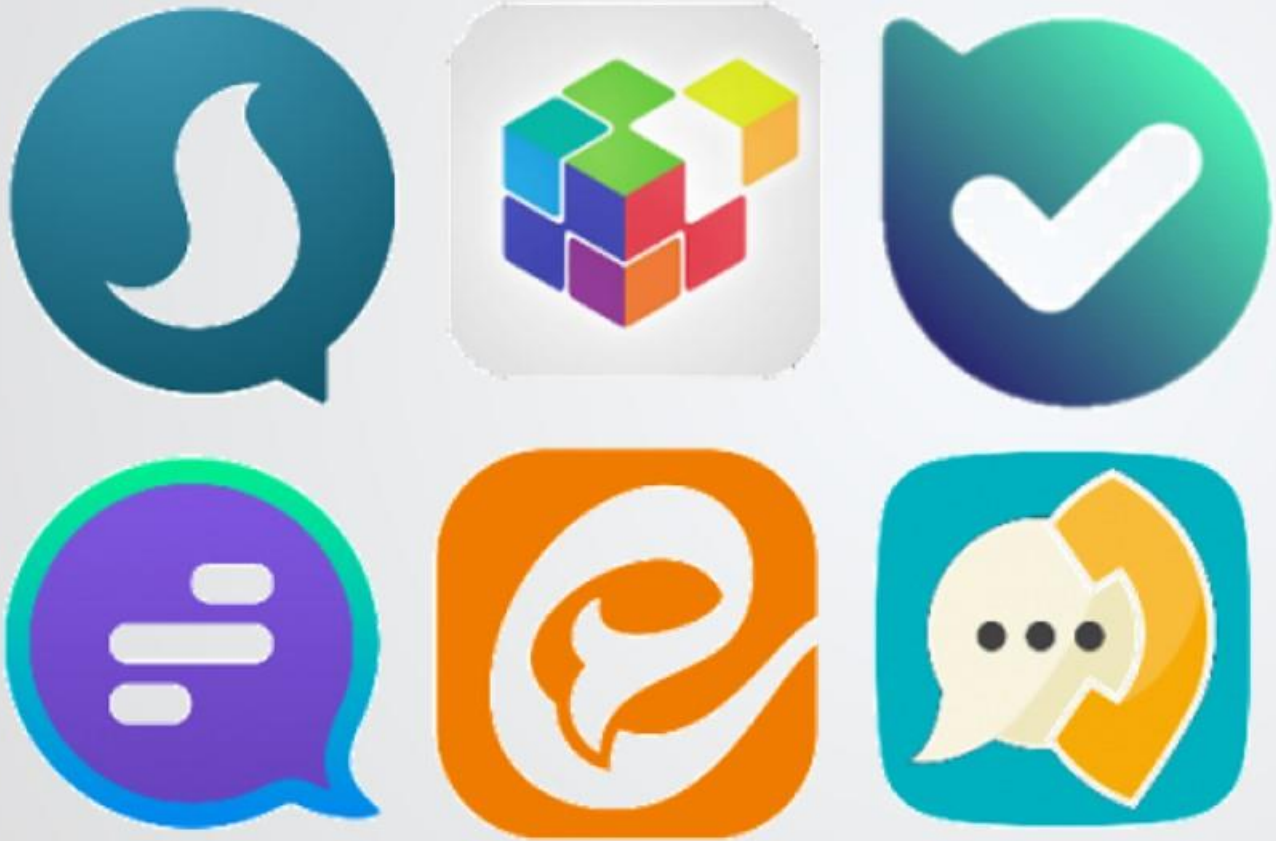
جرائم متاثر از نقض حریم خصوصی

- کلاهبرداری
- مزاحمت اینترنتی
- هتک حیثیت
- انتشار تصاویر خصوصی
- اخاذی

انتشار تصاویر خصوصی در فضای مجازی

آشنایی با خطرات و راهکارهای پیشگیری از انتشار
تصاویر خصوصی در فضای مجازی

حذف تصاویر خصوصی از شبکه اجتماعی



گزارش تخلف

شکایت قضایی

حذف تصاویر خصوصی از شبکه اجتماعی

گزینه "گزارش" یا Report

گزینه "این حساب کاربری من است" یا Someone is pretending to be me

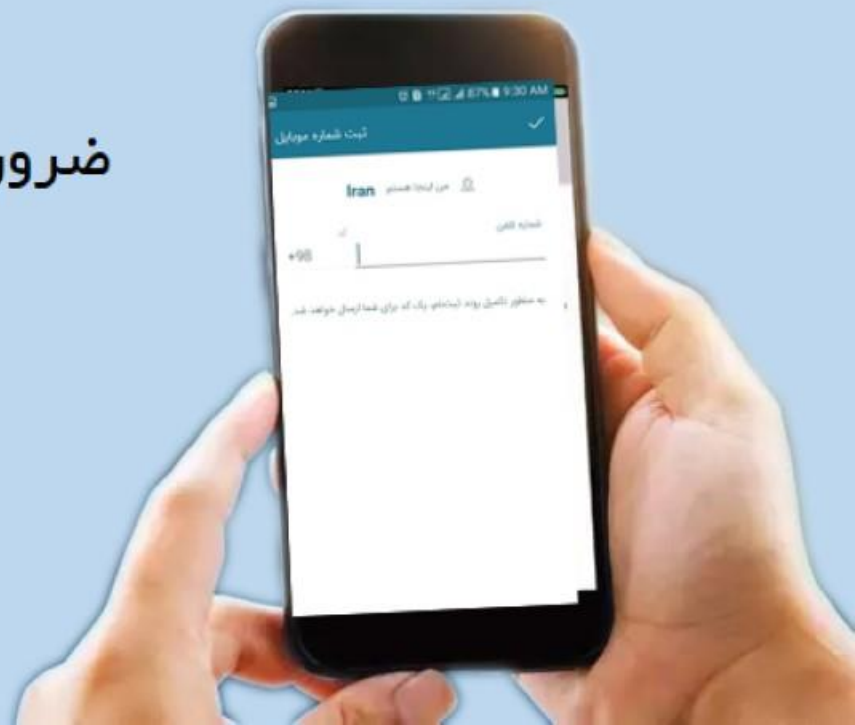
احزار هویت

گزارش همزمان

بسم الله الرحمن الرحیم

امن سازی پیامرسان های موبایلی

ضرورت توجه به امن سازی پیام رسان ها و راهکارهای
امن سازی پیام رسان های ایرانی



چهار کار مهم برای امن سازی پیامرسان!!

فعالسازی قفل

فعالسازی رمز تایید
دو مرحله‌ای

نشست های فعال

تنظیمات
حریم خصوصی

فعالسازی قفل پیام رسان

۱ تنظیمات

۲ حریم خصوصی و امنیت

۳
امنیت
قفل با گذرواژه
تأیید دو مرحله‌ای غیرفعال
دستگاه‌ها

۴
قفل با گذرواژه
تغییر گذرواژه

فعالسازی تایید دو مرحله ای

۱ تنظیمات

۲ حریم خصوصی و امنیت

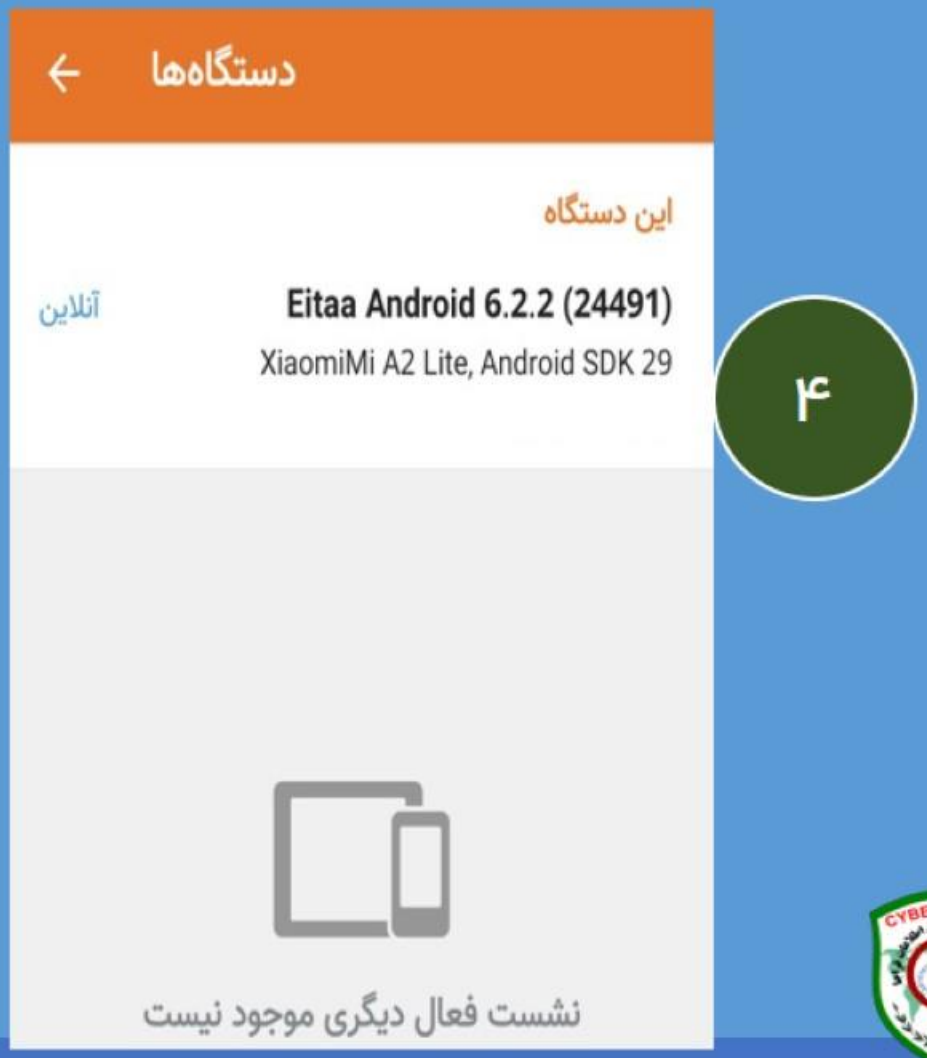
۳
امنیت
قفل با گذرواژه
تأیید دو مرحله‌ای غیرفعال
دستگاه‌ها

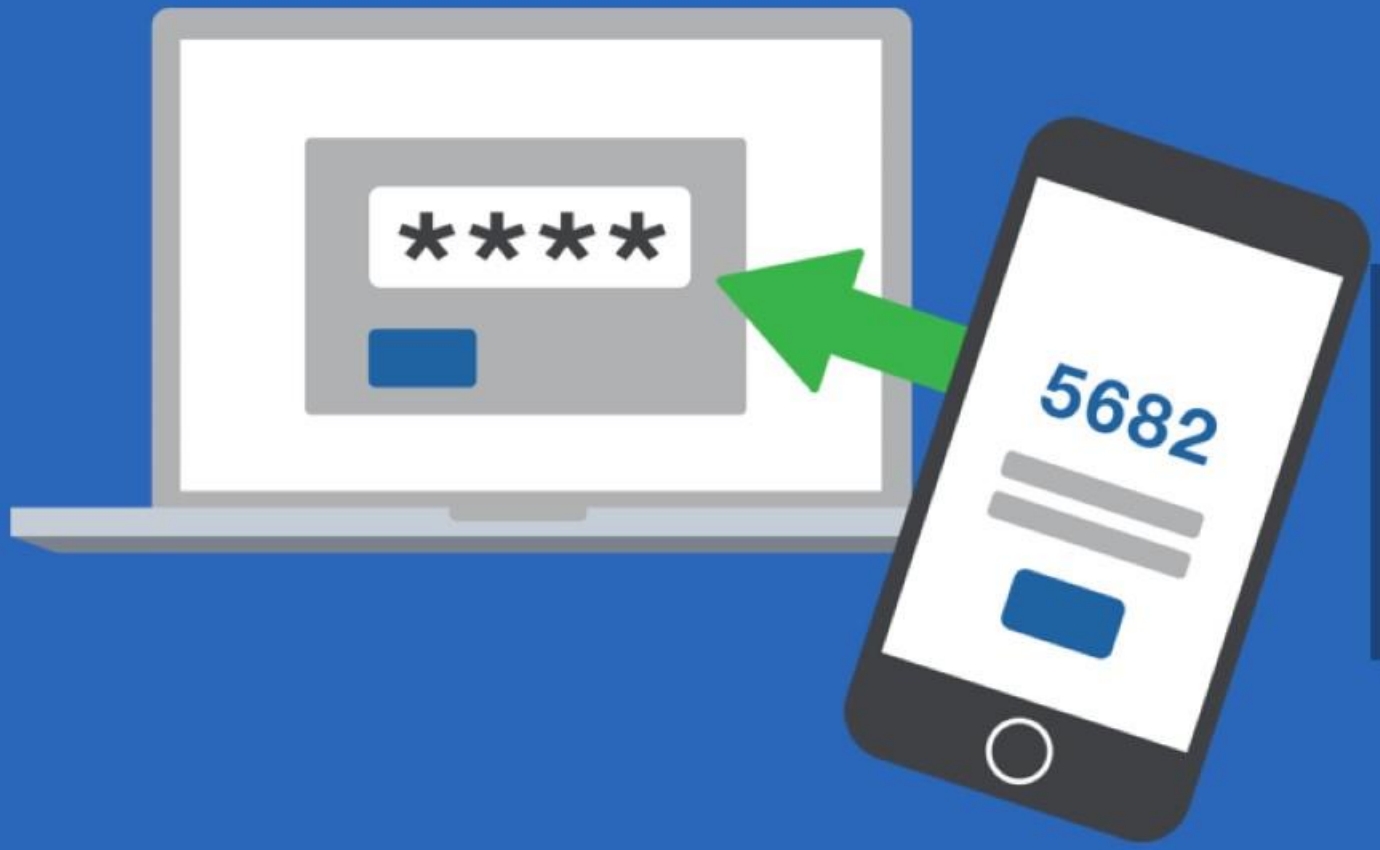
۴
تنظیم گذرواژه اضافی
شما می‌توانید گذرواژه‌ای تنظیم کنید که هنگام ورود به حساب کاربری خود در یک دستگاه جدید، علاوه بر کدی که از طریق پیامک دریافت می‌کنید، از شما خواسته می‌شود.

۵
پین
یک گذرواژه وارد کنید

۶
ایمیل شما
********@gmail.com

نشست های فعال





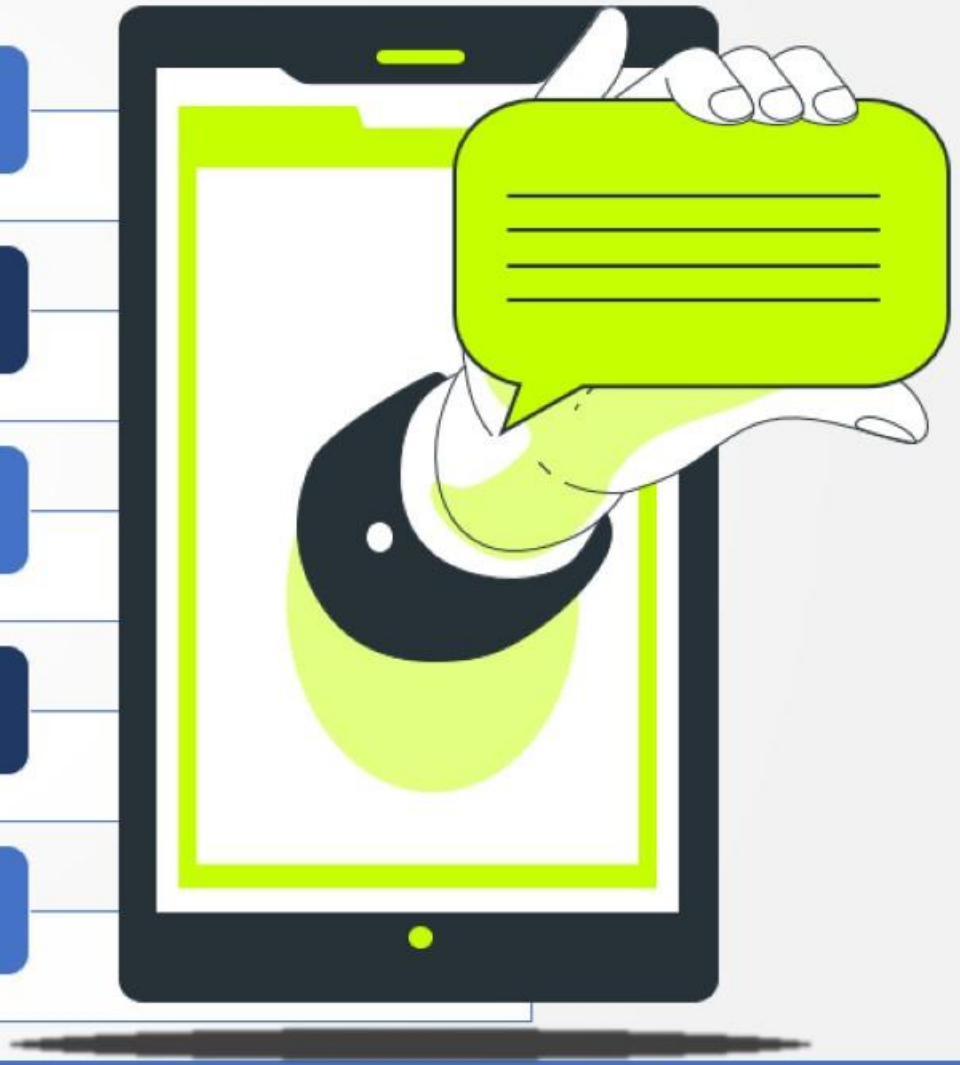
به هیچ وجه کد تایید هویت یا فعال سازی را برای کسی ارسال نکنید

شش اقدام بعد از هک شدن پیام رسان

- بررسی نشست های فعال
- مستند سازی نشست های فعال
- غیر فعال کردن دستگاه غیر مجاز
- اطلاع رسانی به دوستان و آشنایان
- حذف برنامه های جعلی
- پیگیری قضایی و گزارش به پلیس فتا

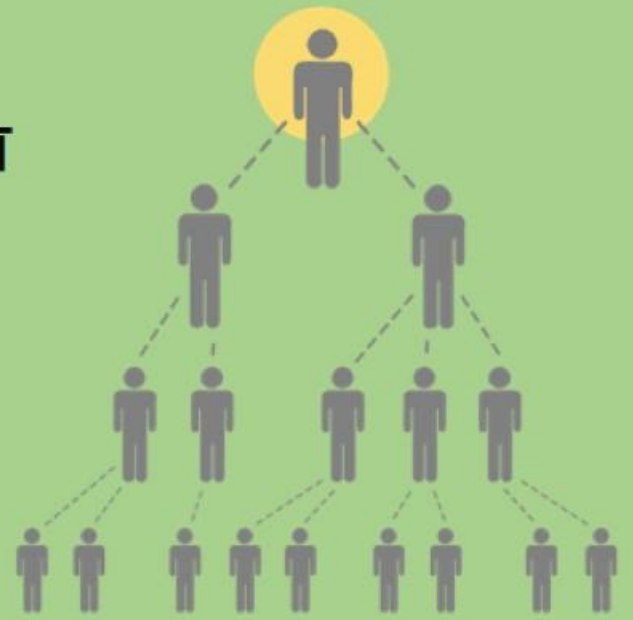
توصیه های مهم در استفاده امن از پیام رسان ها

- پیام رسان را از فروشگاه های معتبر دریافت و نصب کنید
- کدهای فعال سازی VERIFY CODE را برای کسی ارسال نکنید
- مراقب لینک هایی که در گفتگوهای آنلاین دریافت می کنید باشید
- از گوشی خود با استفاده از نرم افزار امنیتی محافظت کنید
- پیام رسان های خود را همیشه به روزرسانی کنید



کلاهبرداری جذب سرمایه

آشنایی با شگردهای کلاهبرداری از طریق جذب سرمایه در فضای مجازی



شگردهای کلاهبرداری جذب سرمایه

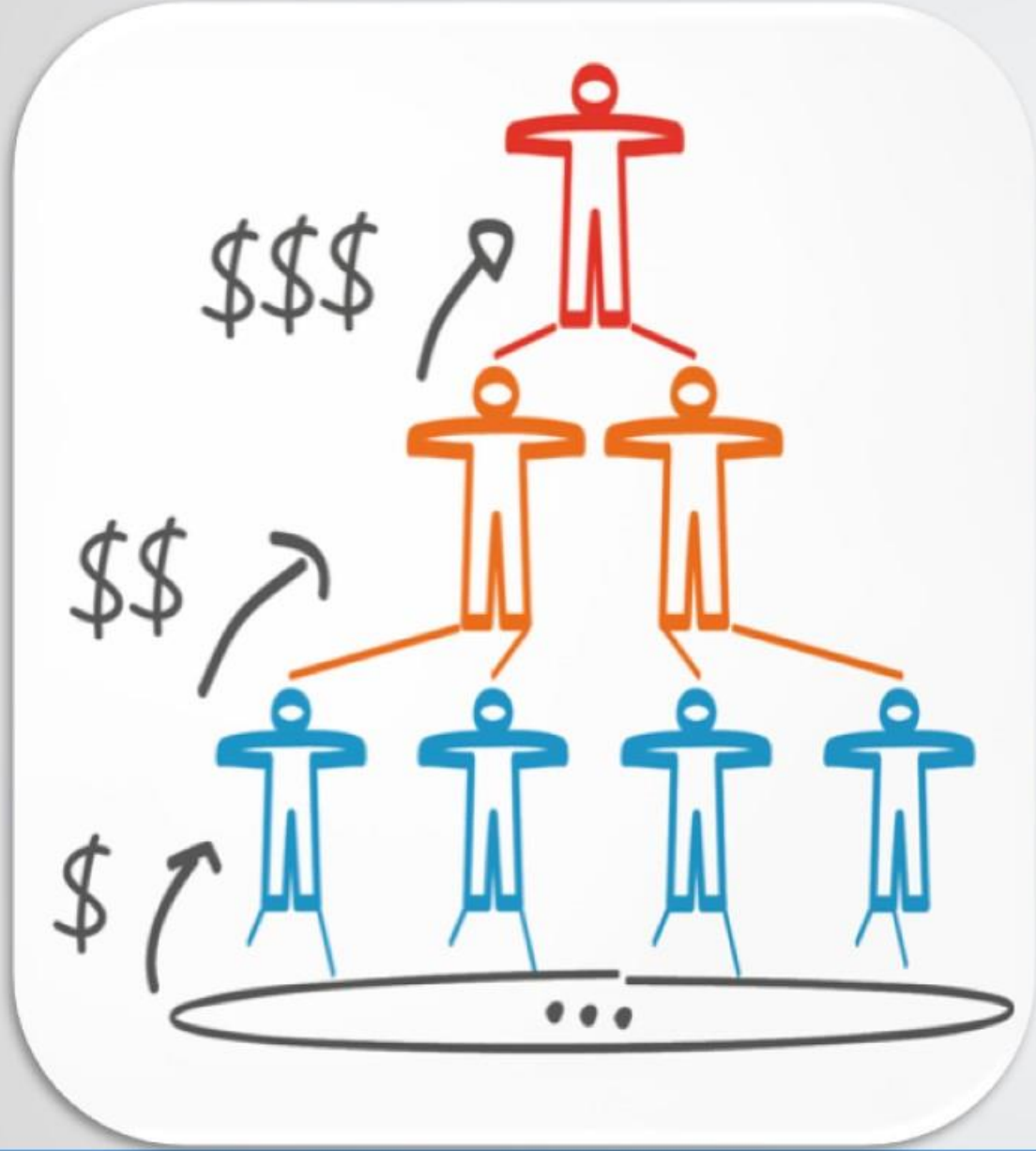
سرمایه گذاری هرمی

فروش توکن های بی ارزش

فروش توکن‌های جعلی

خیریه های جعلی

۱ – سرمایه گذاری هرمی



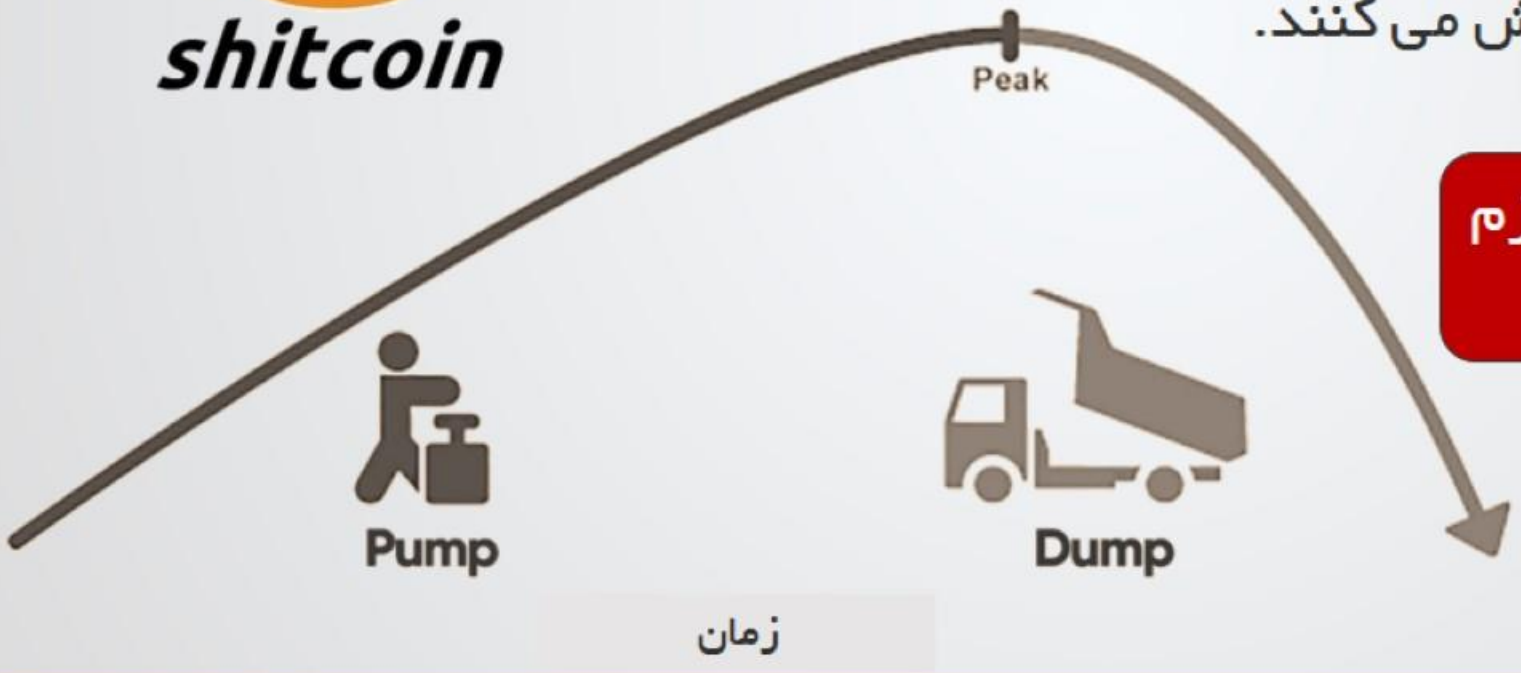
- فریب با وعده سودهای عالی
- فریب با وعده چند برابر شدن سرمایه
- پرداخت های ابتدایی
- ایجاد سازوکار اعتبار جعلی
- فروریزی یک شبه شبکه

هیچ راهی برای یک شبه پولدار شدن وجود ندارد.

۲ – فروش رمزارزهای بی ارزش

- از لحاظ فنی کاملا یک رمزارز محسوب می شوند.
- با تبلیغات بدون پشتوانه قیمت سازی می شوند.
- بعد از مدت کوتاهی سقوط ارزش می کنند.

بدون دانش فنی و اقتصادی لازم وارد بازار رمزارزهای نشوید.



۳- فروش رمزارزهای جعلی

- فروش رمزارزهای جعلی به افراد نا آگاه
- فروش در قالب صرافی های جعلی

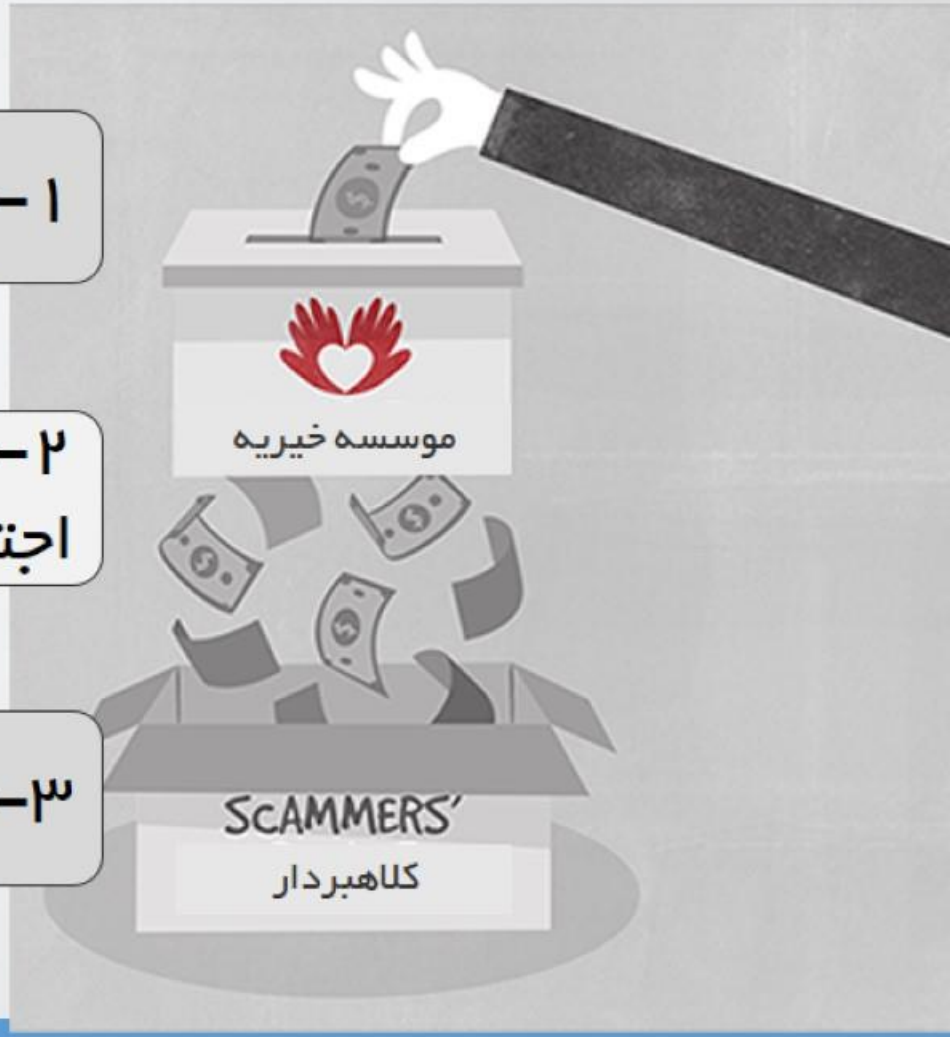
بدون دانش فنی و اقتصادی لازم وارد بازار رمزارزهای نشوید.

۴- خیریه های جعلی

۱ – موسسات خیریه جعلی

۲- افراد شیادی که در شبکه های اجتماعی درخواست کمک می کنند.

۳- بیوه های میلیاردر در حال مرگ



کلاهبرداری پیامکی

آشنایی با شگردهای کلاهبرداری از طریق ارسال پیامک
های جعلی در فضای مجازی

چرخه کلاهبرداری از طریق پیامک

پیامک های جعلی

ارسال پیام از شماره شخصی

متن پیام رسمی نیست و ترغیب به انجام کاری

دارای لینک برای هدایت به صفحه جعلی

پیامک های جعلی

ارسال پیام از شماره شخصی

+989356[redacted]

افزودن به مخاطبین | انسداد شماره

یکشنبه ۲۳ آوریل ۲۰۲۳

پروَنده شما به شماره رهگیری 10384 به شعبه دادسَرای اِنقلاب بازپرسی2 ارجاع شد.
پیگیری ازطریق پیوند زیر:
veryshort.ir/352d4

۲۱:۴۳

+989100[redacted]

پنجشنبه ۲۹ ژوئیهٔ ۲۰۲۱, ۱۴:۴۶

هزینه سامانه الکترونیکی ثنا ابتدا فیلتر شکن دستگاه خود را روشن کرده و از طریق لینک زیر اقدام‌نمایید.
درغیراین صورت طبق ماده523قانون اساسی رای قطعی صادر و اجرا خواهد شد.
شعبه3بازپرسی دادسرای ناحیه2

هزینه ثبت (2/000تومان)

http://urly.ir/EO5al

متن پیام رسمی نیست و ترغیب به انجام کاری

لینک کوتاه شده برای گمراه کردن کاربر

سرشماره اسمی

پیامک‌های مربوط به سامانه‌های قوه‌قضاییه مانند ثنا، ابلاغ، نظرسنجی، اطلاع رسانی، دادرسی الکترونیک و ...

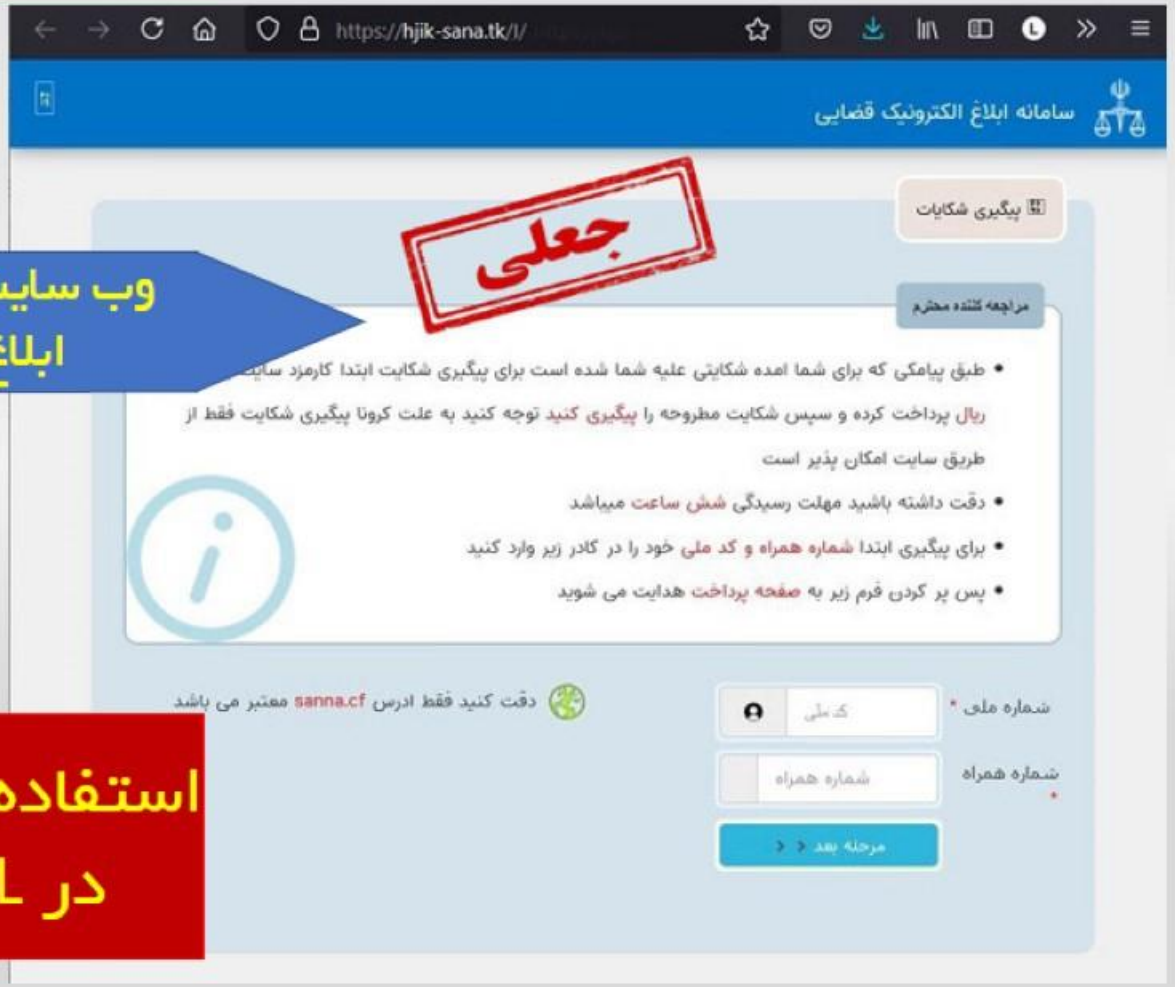
بدون شماره و فقط با نام ADLIRAN ارسال می‌شود.

به پیامک‌هایی که بدون نام و از سرشماره‌های ناشناس ارسال شده و حاوی پیام‌هایی با موضوع پرونده قضایی یا حاوی لینک است اعتنا نکرده، وارد لینک‌های اعلامی نشوید.

وب سایت های جعلی

lp.thelatinapro.com/NewSaham/

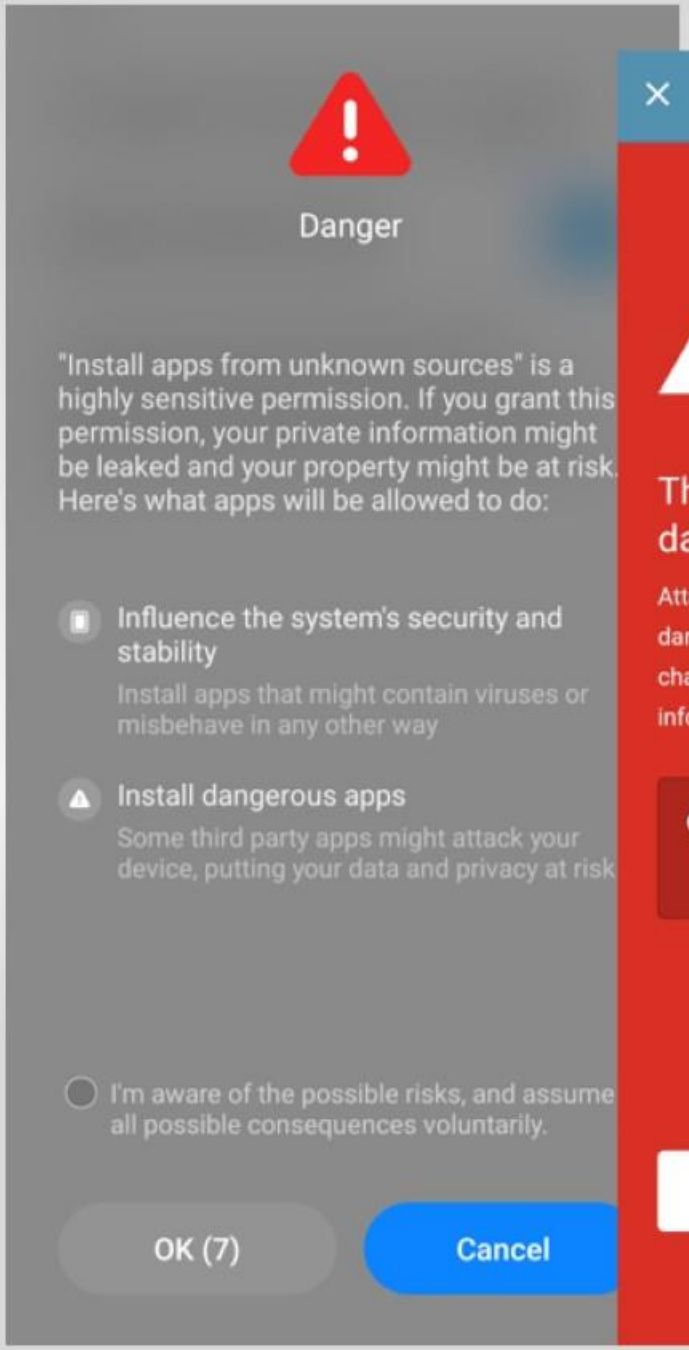
وب سایت جعلی سهام عدالت

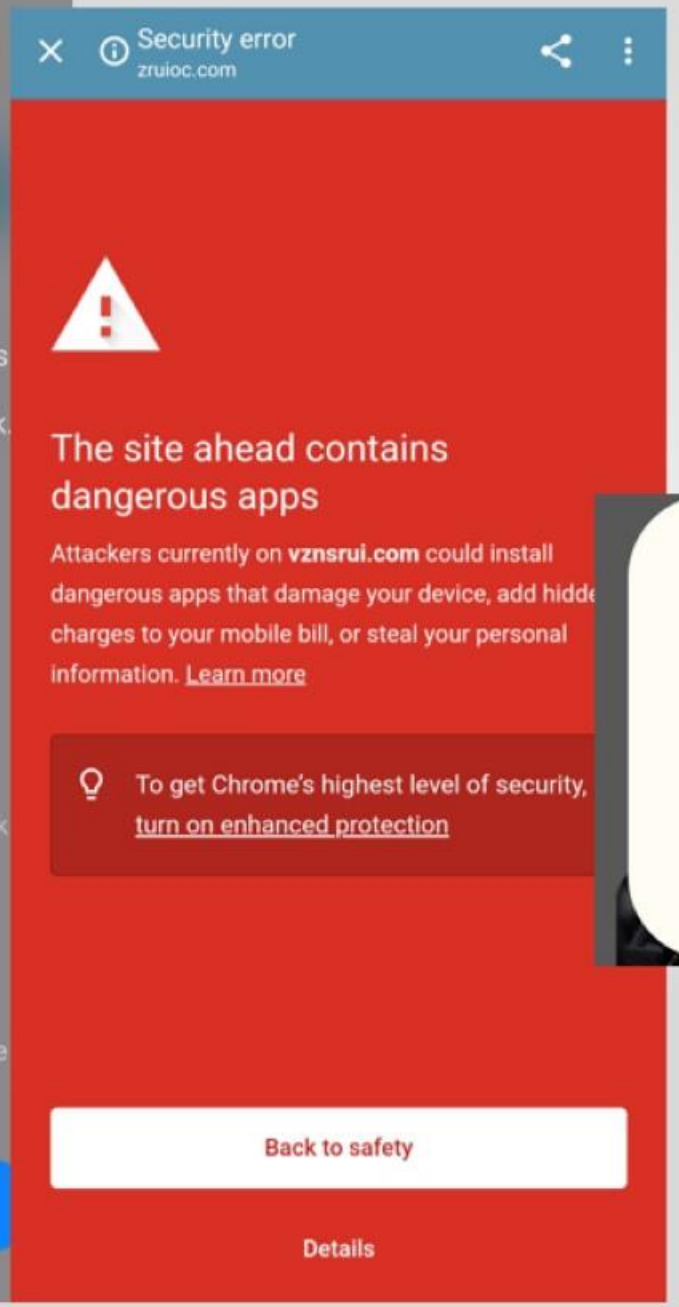


وب سایت جعلی سامانه ابلاغ اوراق قضایی

استفاده از آدرس نامعتبر در URL وب سایت

دریافت اپلیکیشن جعلی





هشدار امنیتی نصب برنامه نا ایمن

درگاه پرداخت جعلی

pt-op.tk/p2/843525/index.php

به آدرس shaparak.ir دقت کنید

استفاده از آدرس جعلی

قبل از وارد کردن رمز پویا اطلاعات پیامک

دریافتی را با درگاه وتراکنش خود تطبیق دهید

بانک [redacted]
نوع تراکنش:خرید
آسان پرداخت پرشین
مبلغ:12,000
تاریخ:1400/06/[redacted]
ساعت:10:16:51
شماره کارت:[redacted]16
رمز یکبار مصرف(پویا):59225
از در اختیار قرار دادن محتویات این پیامک به دیگران جدا خودداري فرمایید

پنج توصیه نجات بخش

1. پیامک های اطلاع‌رسانی مربوط به سازمان‌ها با سرشماره های اسمی ارسال می گردد.
2. هرگونه پیامک خدماتی از سرشماره های شخصی نامعتبر است.
3. به آدرس وب سایت ها، متن پیامک دریافتی و هشدارهای امنیتی مرورگر توجه کنید.
4. تمامی درگاه های بانکی به دامنه SHAPARAK.IR ختم می شوند.
5. در صورت دریافت پیامک مشکوک از طریق شماره ۰۹۶۳۸۰ با کارشناسان پلیس فتا مشورت کنید.

خروج از بحران

- قطع اینترنت تلفن همراه
- حذف برنامه جعلی
- تخلیه حساب بانکی از خودپرداز
- اطلاع رسانی به دیگران
- گزارش به پلیس فتا
- پیگیری قضایی

بسم الله الرحمن الرحیم

کلاهبرداری در بسترسایت های ثبت آگهی

آشنایی با راهکارهای پیشگیری از کلاهبرداری در بستر سایت های ثبت آگهی در فضای مجازی

انواع کلاهبرداری در سایت های ثبت آگهی

۱ دریافت بیعانه

۲ کلاهبرداری مثلثی

۳ رسیدساز جعلی

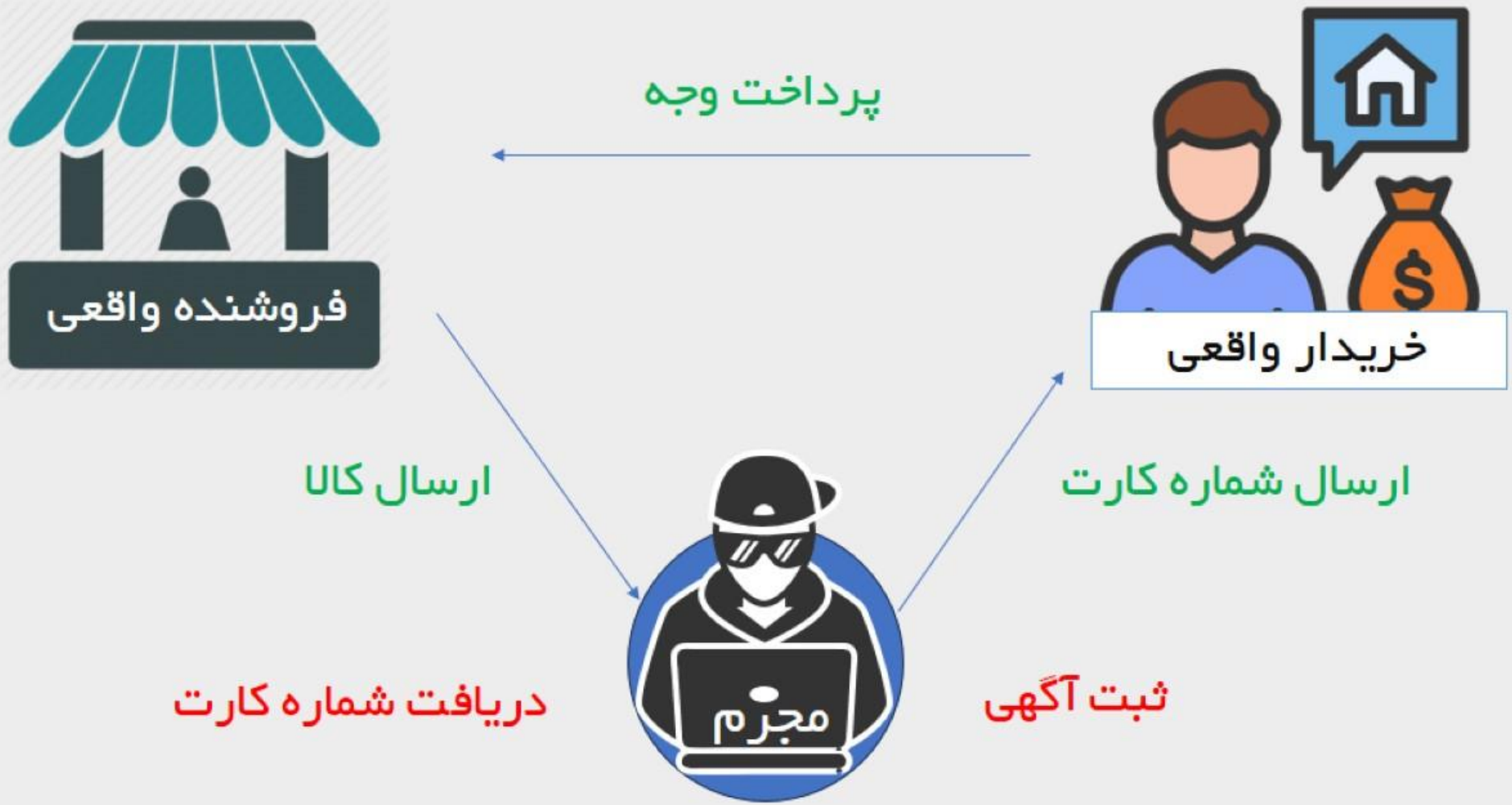
۴ کار در منزل

۵ جذب حمایت اجتماعی

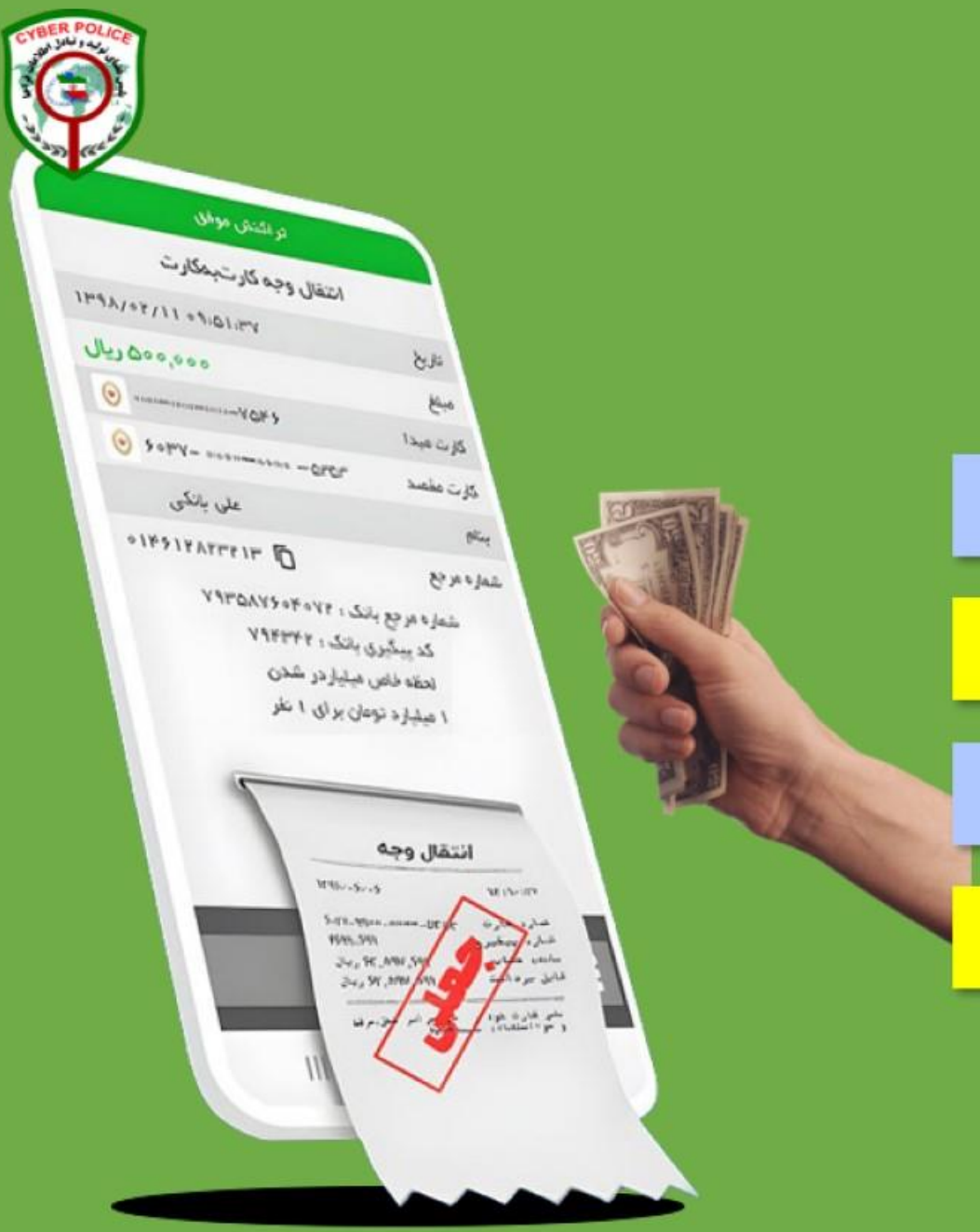
۱ – کلاهبرداری دریافت بیعانه

تنها در صورت رویت کالا و به صورت حضوری پول پرداخت کنید.

۲- کلاهبرداری مثلثی



۳- رسید ساز جعلی



۱ – حتما پیامک بانکی کارت خود را فعال کنید.

۲ – حتما موجودی حساب خود را بررسی نمایید.

۳- پس از تایید واریز وجه کالا را تحویل دهید.

۴- مبالغ بالا را در محل امن و با همراه پرداخت کنید.

۴- کلاهبرداری کار در منزل

تبلیغ کار در منزل در سایت های آگهی و شبکه های اجتماعی

فریب در قالب دورکاری در مشاغلی مانند حسابدار، بازیاب، مدیرفروش، بسته بندی و...

دسترسی به کارت بانکی و به اینترنت بانک قربانی

تبادل مالی با حساب قربانی و انتصاب جرم به او

راه‌های پیشگیری از کلاهبرداری کار در منزل

اگر آگهی کار در منزلی را مشاهده کردید که شرایطی از قبیل

- پرداخت حقوق بسیار بالا
- عدم نیاز به تخصص یا مهارت
- عدم نیاز به رزومه کاری
- نیاز به واریز وجه به عنوان پیش پرداخت

احتمال کلاهبرداری در آن زیاد است

راه‌های پیشگیری از کلاهبرداری کار در منزل

از آگهی‌های غیرواقعی و وسوسه انگیز پرهیز کنید

اطلاعات شخصی خود را در اختیار افراد ناشناس قرار ندهید

فقط به خاطر دعاهای برجسته، به آن‌ها اعتماد نکنید

قبل از هرگونه پرداخت، اطلاعات شرکت یا سازمان مورد نظر را به دقت بررسی کنید

قبل از انتخاب هر فرصت کاری، تحقیق کاملی انجام دهید.

از واریز پول به حساب شخص حقیقی خودداری کنید

با پیروی از این موارد ساده، می‌توانید خود را از بسیاری از کلاهبرداری‌های مرتبط با کار در منزل محافظت کنید

۵- جذب حمایت اجتماعی

ثبت آگهی با موضوعات جذب حمایت اجتماعی توسط کلاهبرداران اینترنتی

- خیریه
- جذب سرمایه
- بیماران
- مشارکت شغلی

پرداخت بیعانه در معامله پرخطر است.

تا به اصالت کالا و جزئیات آن اطمینان پیدا نکرده اید معامله نکنید.

از روش های تضمین معامله استفاده کنید.

معامله حضوری را بر هر شیوه دیگری ترجیح دهید

به هویت طرف معامله خود دقت کنید

شگردهای مجرمان در اربعین

- کلاهبرداری درخواست قرض
- کلاهبرداری جمع آوری نذورات
- کلاهبرداری با دریافت بیعانه
- اسکیمر
- لینک های جعلی

کلاهبرداری درخواست قرض

در مسیر راهپیمایی پولم تمام شده

در مسیر تصادف کردم پول نیاز دارم

کارت بانکی من دچار مشکل شده

قبل از واریز تماس بگیرید

کلاهبرداری جمع آوری نذورات

خیرین عزیز مراقب باشید

کمپین های خیریه

کلاهبرداران سایبری به روش های مختلف از قبیل ایجاد اکانت های جعلی یا تبلیغات در فضای مجازی و سوء استفاده از عناوین موسسه های خیریه معتبر و بدنبال آن، انتشار شماره کارت های بانکی اقدام به فریب کاربران و اخذ کمک های نقدی آنها می کنند.

- در راه ماندگان دروغین
- موکب های جعلی
- بیمارنما ها

کمک های خود را از راه های مطمئن انجام دهید

پرداخت بیعانه

آگهی خودروی کرایه در سایت های ثبت آگهی

فروش وسایل سفر

به هیچ وجه بیعانه پرداخت نکنید

اسکیمر

دست فروشان بین راهی

فروشندگان دوره گرد

فروشندگان غیر مجاز ارز

به سلامت کارت خوان توجه کنید

رمز کارت را خودتان وارد کنید

کارت پرداخت خرد داشته باشید

اسکیمر

credit card skimming device

تشخیص کارتخوان واقعی از جعلی

- روش بون صفحه کارت خوان
- درج شدن نام فروشگاه روی کارتخوان
- مشخص بودن فرآیند اتصال و دریافت اطلاعات

لینک های جعلی

- خرید ارز اربعین
- اینترنت رایگان اربعین
- دریافت گذرنامه
- برنده شدن در رادیو اربعین

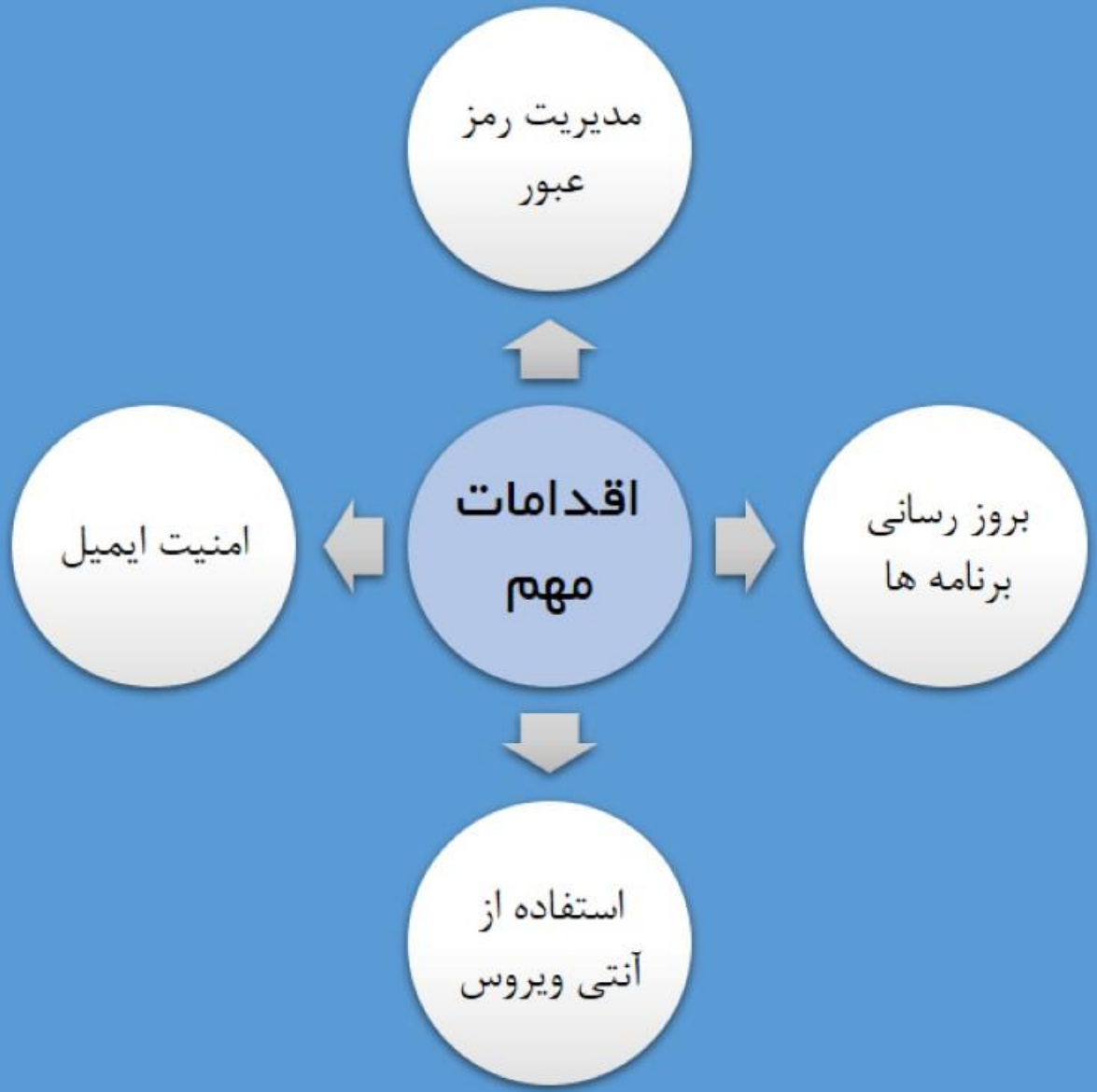
به هیچ وجه لینک های مشکوک پیامک شده و دریافت شده در پیامرسان ها را بازنکنید

بهداشت امنیت سایبری

آشنایی با مجموعه راهکارهای حفظ سلامت و امنیت
کاربران، دستگاه ها، شبکه ها و داده ها

بهداشت امنیت سایبری چیست؟

به مجموعه اقداماتی گفته می شود که کاربران رایانه و موبایل برای حفظ ایمنی و امنیت اطلاعات و سیستم‌های خود در یک محیط آنلاین باید بکار بگیرند.



اقدامات مهم برای امنیت سایبری

۱ – مدیریت رمز عبور

- ترکیب حروف بزرگ + حروف کوچک + عدد + نشانه
- طول ۱۴ کاراکتر یا بیشتر

اشتباهات رایج در امنیت رمز عبور

۱ استفاده مجدد از رمزهای عبور

۲ استفاده از ترکیبات ساده رمز

۳ استفاده از کلیدهای کنار هم در صفحه کلید

۴ استفاده از اطلاعات شناسنامه ای

۵ استفاده از شبکه های وای فای ناامن در مکان های عمومی

۶ استفاده از احراز هویت چند عاملی

۷ به اشتراک گذاری رمز

۲– به روز رسانی برنامه ها

استفاده از آسیب پذیری نرم افزارها از مهمترین روش های هک و دسترسی به اطلاعات کاربران است.

- تنظیم به‌روزرسانی‌ها برای اجرای خودکار
- به‌روزرسانی‌ها از منابع معتبر
- جایگزینی نرم افزارهای منسوخ یا پشتیبانی نشده

۳- استفاده از آنتی ویروس

به روز نگاه دارید

به هشدارها توجه کنید

جویش کنید

استفاده از برنامه های ضد ویروس و دیواره های آتش از مهمترین اقدامات برای حفظ امنیت داده و تجهیزات است.

۴– امنیت ایمیل

نقش امنیت ایمیل در امنیت حریم خصوصی

- حساب کاربری شبکه های اجتماعی با ایمیل راه اندازی می شوند.
- کلمه عبور حساب کاربری شبکه های اجتماعی با ایمیل بازنشانی Recovery می شوند.
- ایمیل محل نگهداری اطلاعات بسیار مهم کاربران است.
- ایمیل بستر ارتباط

توصیه مهم

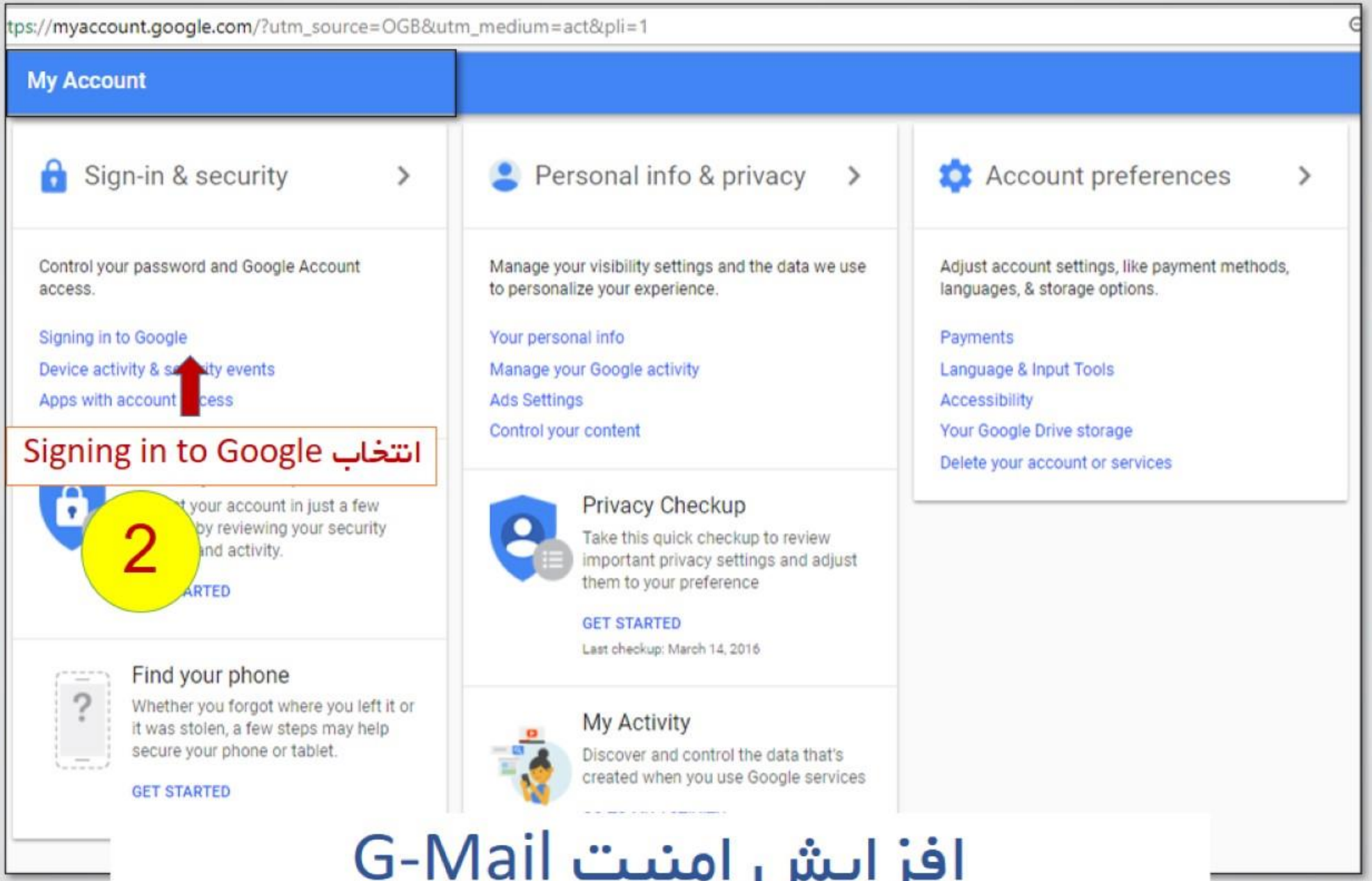
- حداقل سه ایمیل داشته باشید

- ایمیل برای امور شخصی

- ایمیل برای راه اندازی شبکه های اجتماعی

- ایمیل برای وبگردی و کارهای متفرقه

افزایش امنیت G-Mail



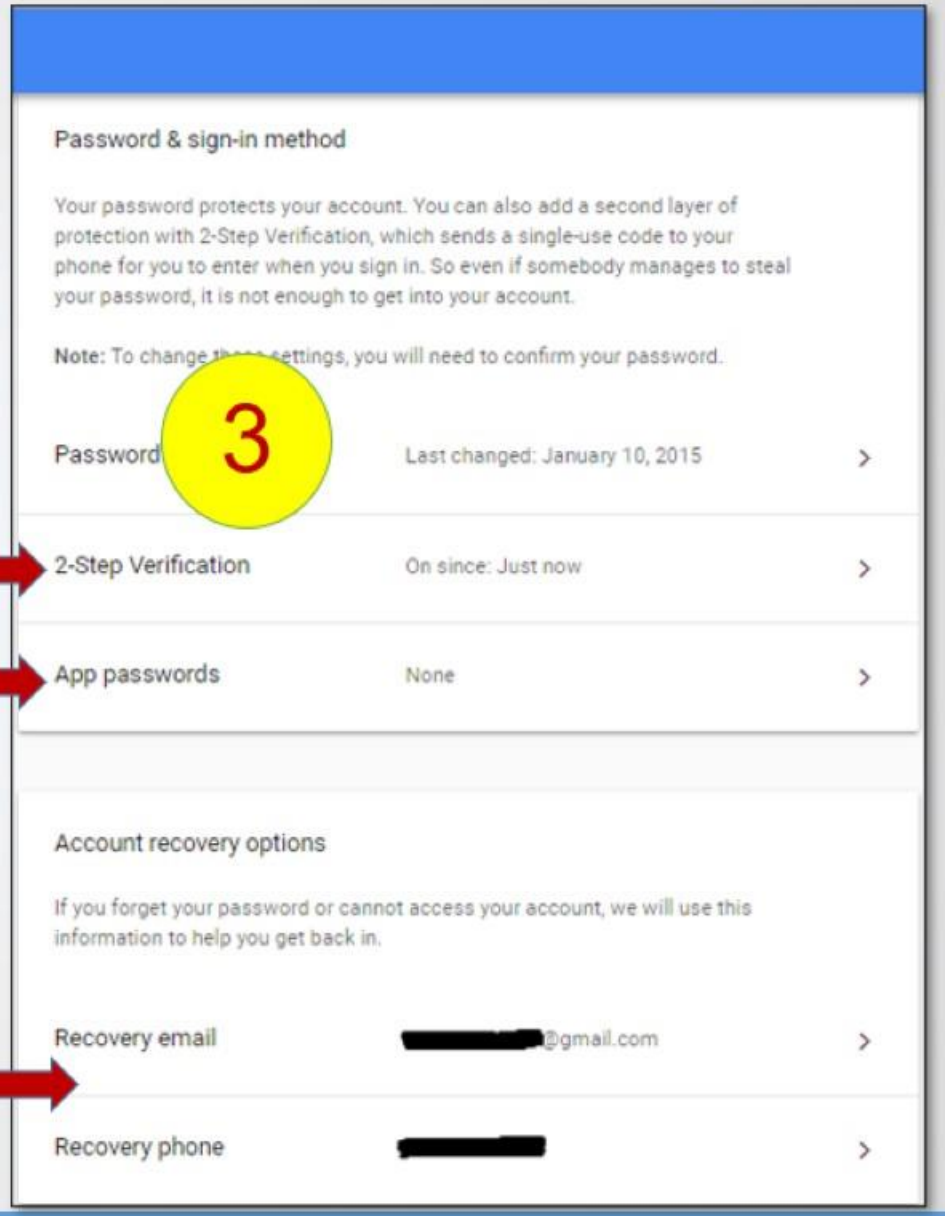
افزایش امنیت G-Mail

افزایش امنیت G-Mail

معرفی شماره موبایل برای ورود ۲ مرحله ای

تایید ورود با موبایل

معرفی Email و شماره موبایل برای بازیابی کلمه عبور



این اشتباهات را مرتکب نشوید

هیچگاه سرویس دهنده ایمیل از شما نمی خواهد تا کلمه عبورتان را از طریق لینک پشتیبان به روز کنید

تا جای ممکن از محل های عمومی و کافی نت ها برای چک کردن ایمیل های خود استفاده کنید

پس از پایان کار تان با ایمیل از آن Sign out کنید

برای ایمیل ها و حساب های کاربری خود در شبکه های اجتماعی از کلمه عبور مشابه استفاده نکنید

در باز کردن پیوست ایمیل های ناشناس دقت کنید