

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



امن سازی پیام رسانی های موبایلی

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



انتشار تصاویر خصوصی در فضای مجازی

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



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



کلاهبرداری در بسترسایت های ثبت آگهی

آشنایی با راهکارهای پیشگیری از کلاهبرداری در بسترسایت 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 منافی 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 تأمل به اشتراک‌گذاری اطلاعات پرداخته و از خدمات آنلاین استفاده می‌کنند



جرائم متاثر از نقض حریم خصوصی

کلاهبرداری

مزاحمت
ایترتی

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





هدف 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

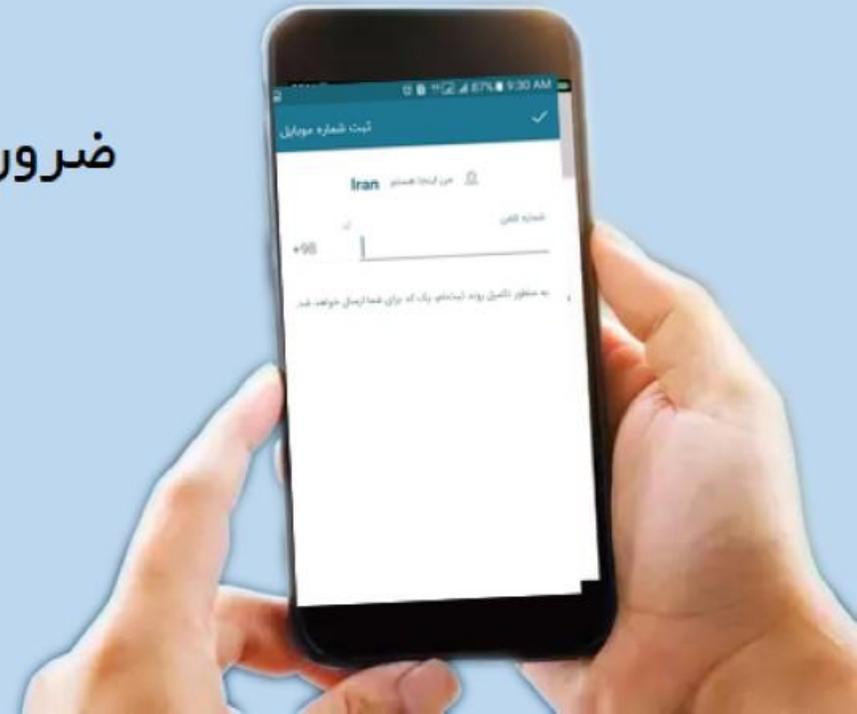
گزارش همزمان

بِسْمِ
الرَّحْمَنِ
الرَّحِيمِ



امن سازی پیام رسان 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 رمز تایید
دو مرحله‌ای



فعالسازی قفل



تنظیمات
حریم خصوصی



نشست های فعال



فعالسازی قفل پیام رسان



تنظیمات

۱

حریم خصوصی و امنیت



۲

امنیت

قفل با گذرواژه

۳

غیرفعال

تأیید دو مرحله‌ای

دستگاهها



قفل با گذرواژه

تغییر گذرواژه

۴



فعالسازی تایید دو مرحله ای



تنظیمات

۱



حریم خصوصی و امنیت

۲

امنیت

قفل با گذرواژه

۳

تأیید دو مرحله‌ای

غیرفعال

دستگاه‌ها

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.

۴

← پین ▾ ✓

یک گذرواژه وارد کنید

۵

ایمیل شما

*****@gmail.com

۶





تنظیمات

۱

حریم خصوصی و امنیت



۲

امنیت

قفل با گذرواژه

۳

غیرفعال

تأیید دو مرحله‌ای

دستگاه‌ها

نشست های فعال

← دستگاه‌ها

این دستگاه

آنلاین

Eitaa Android 6.2.2 (24491)

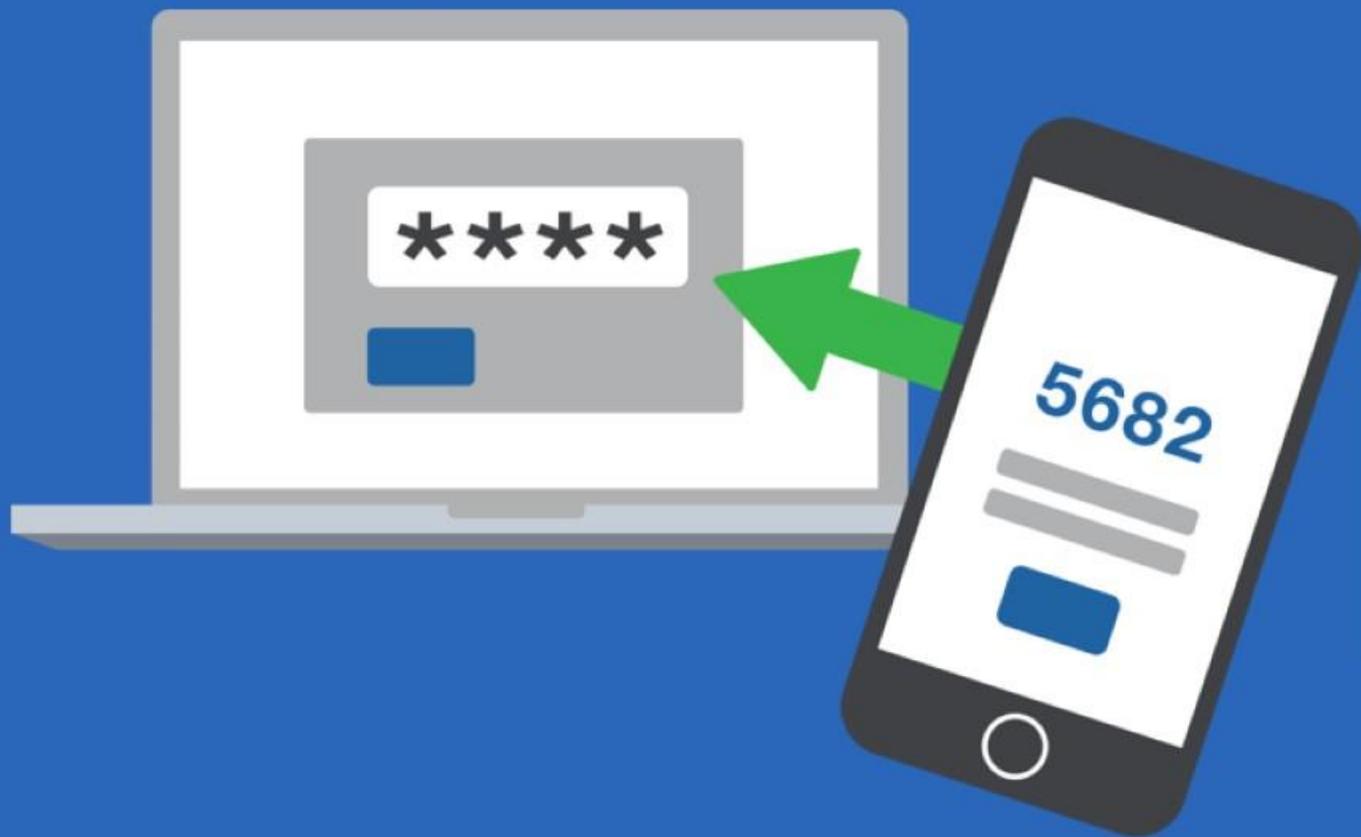
XiaomiMi A2 Lite, Android SDK 29

۴



نشست فعال دیگری موجود نیست





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





شش اقدام بعد از هک شدن پیام رسان

اطلاع رسانی به دوستان و آشنایان

بررسی نشست های فعال

حذف برنامه های جعلی

مستند سازی نشست های فعال

پیگیری قضایی و گزارش به پلیس
فتا

غیر فعال کردن دستگاه غیر مجاز





توصیه های مهم در استفاده امن از پیام رسان ها

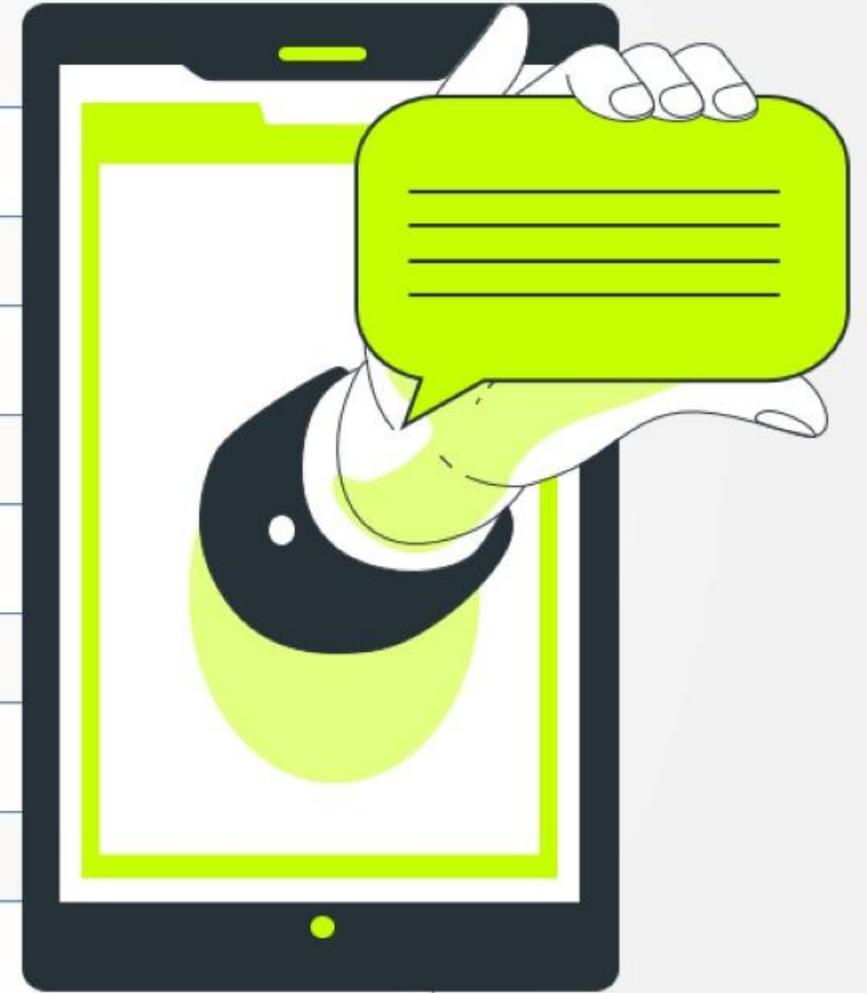
پیام رسان را از فروشگاه های معتبر دریافت و نصب کنید

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

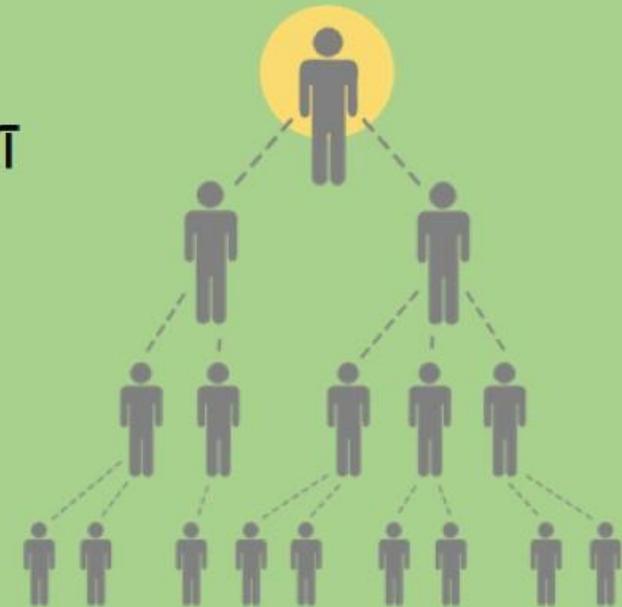
پیام رسان های خود را همیشه به روزرسانی کنید





کلاهبرداری جذب سرمایه

آشنایی با شگردهای کلاهبرداری از طریق جذب سرمایه در فضای مجازی





شگردهای کلاهبرداری جذب سرمایه

سرمایه گذاری هر می

فروش توکن های بی ارزش

فروش توکن های جعلی

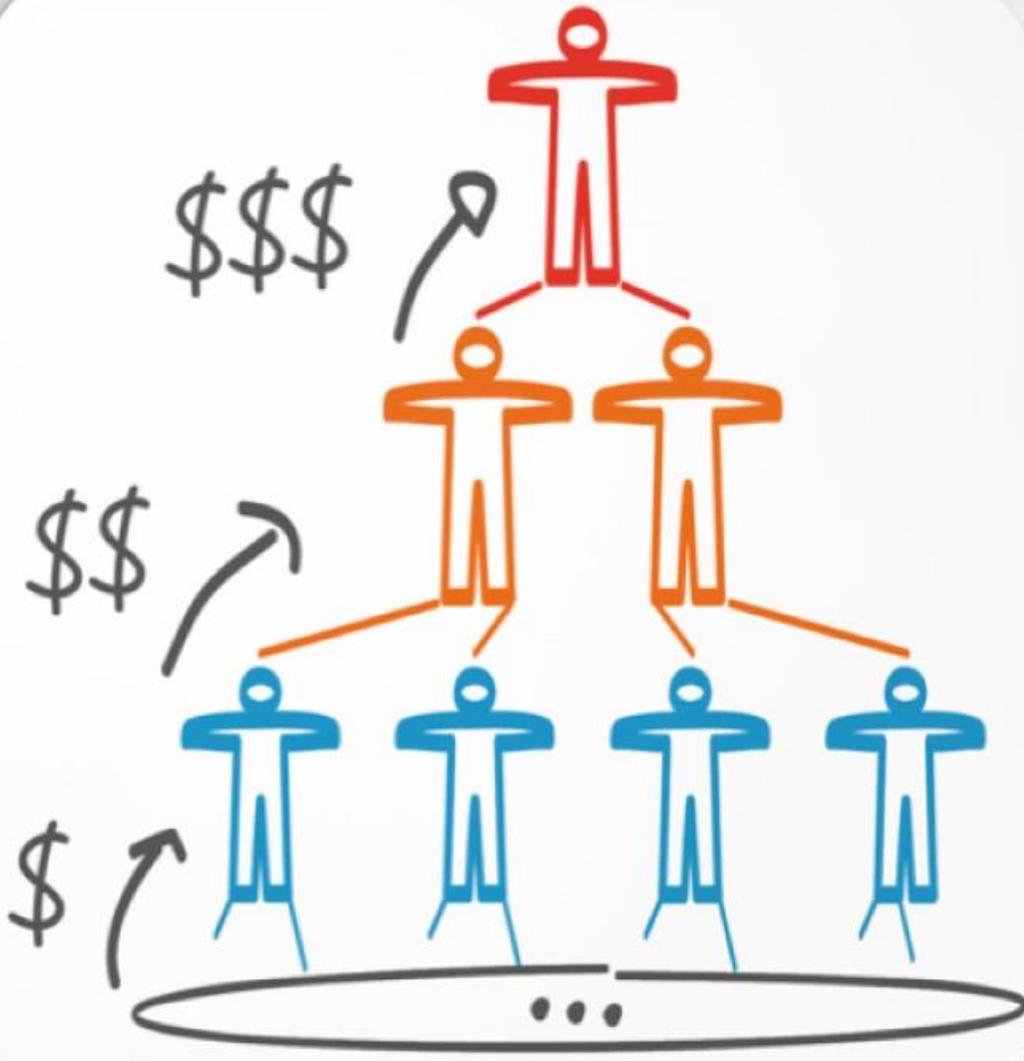
خیریه های جعلی



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.



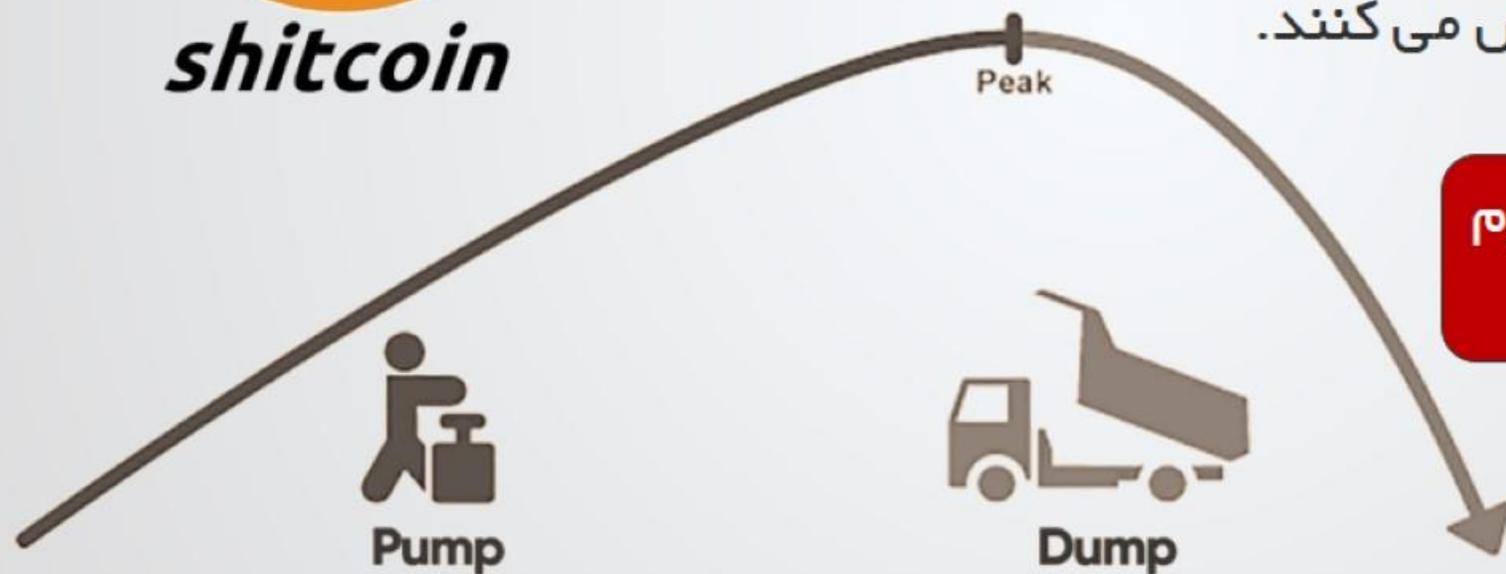
۲ – فروش رمزارزهای بی ارزش



shitcoin

- از لحاظ فنی کاملاً یک رمزارز محسوب می‌شوند.
- با تبلیغات بدون پشتوانه قیمت سازی می‌شوند.
- بعد از مدت کوتاهی سقوط ارزش می‌کنند.

بدون دانش فنی و اقتصادی لازم
وارد بازار رمزارزهای نشوید.



ارزش

زمان

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.

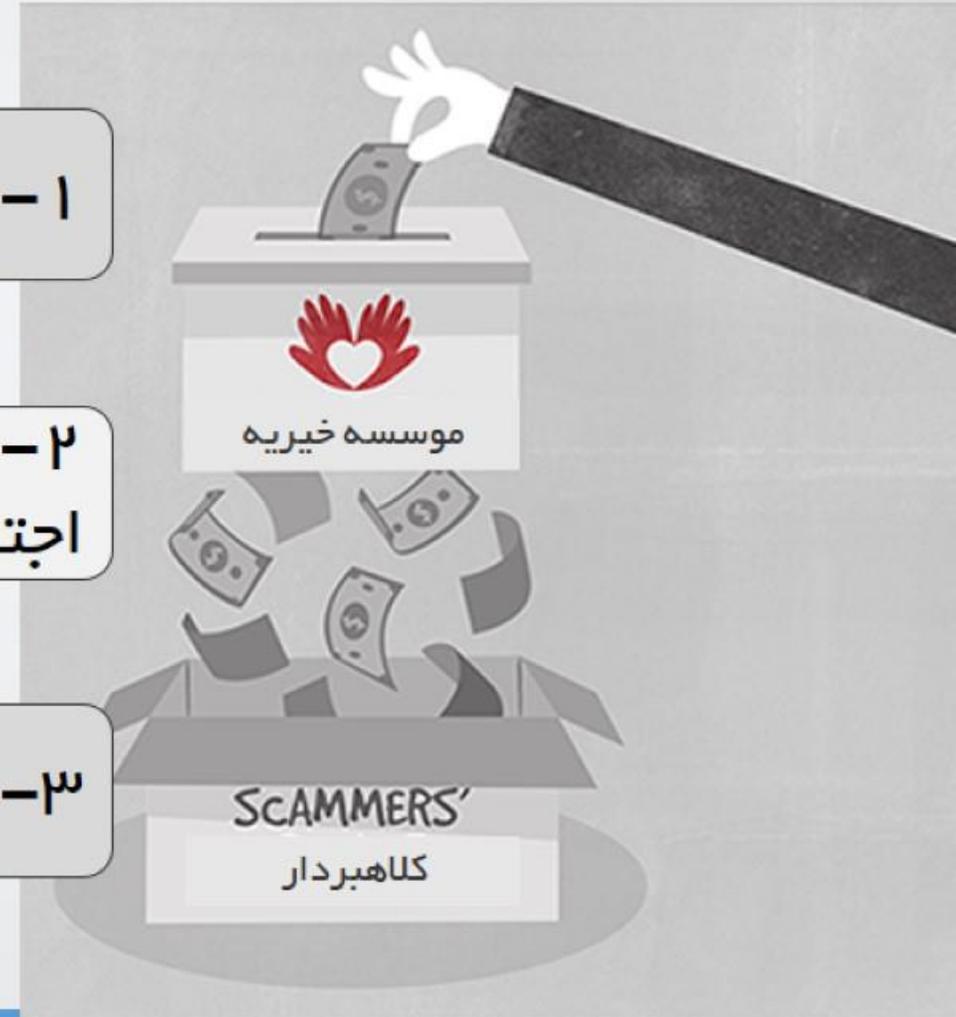


۴- خیریه های جعلی

۱- موسسات خیریه جعلی

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

۳- بیوه های میلیاردی در حال مرگ





کلاهبرداری پیامکی

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





چرخه کلاهبرداری از طریق پیامک



ارسال پیام از شماره شخصی

متن پیام رسمی نیست و ترغیب به انجام کاری

(ابلاغ الکترونیک قضایی)
بنابر شکایتی که علیه شما صورت گرفته و درسایت ثبت شده است برای مشاهده از شکایت خود به سایت زیرمراجعه کنید در غیر این صورت طی (۲۴ ساعت) پرونده به دادگستری ارجاع خواهد شد.

شماره پرونده:
۹۸۳۵۱۱۰۰۳۱۶

آدرس پیگیری : [sana-
adliran.co/Eblagh/
kap018ma91](http://sana-adliran.co/Eblagh/kap018ma91)

دارای لینک برای هدایت به صفحه جعلی

پیامک های جعلی





پیامک های جعلی

ارسال پیام از شماره شخصی

+989356[redacted]

انستاد شماره

افزودن به مخاطبین

۱۵:۰۸ ۵۹% 4G

+989100[redacted]

پنجشنبه ۲۹ ژوئیه ۲۰۲۱، ۱۴:۴۶

یکشنبه ۲۲ آوریل ۲۰۲۳

پرورنده شما به شماره رهگیری **10384** به شعبه دادسرای انقلاب بازپرسی 2 ارجاع شد. پیگیری از طریق پیوند زیر:

veryshort.ir/352d4

۲۱:۲۳



هزینه سامانه الکترونیکی ثنا **ابتدا فیلتر شکن** دستگاه خود را روشن کرده و از طریق لینک زیر اقدام نمایید. درغیراین صورت طبق ماده 523 قانون اساسی رای قطعی صادر و اجرا خواهد شد.

شعبه 3 بازپرسی دادسرای ناحیه 2

هزینه ثبت (2/000 تومان)

<http://urly.ir/E05al>

متن پیام رسمی نیست و ترغیب به انجام کاری

لینک کوتاه شده برای گمراه کردن کاربر



III

○

>



سرشماره اسمی

**پیامک‌های مربوط به سامانه‌های قوه قضاییه
مانند ثنا، ابلاغ، نظر سنجی، 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

Ip.theLatinapro.com/NewSaham/



وب سایت جعلی سهام عدالت

وب سایت جعلی سامانه ابللاغ اوراق قضایی



جعلی

استفاده از آدرس نامعتبر در URL وب سایت



دریافت اپلیکیشن جعلی



Danger

"Install apps from unknown sources" is a highly sensitive permission. If you grant this permission, your private information might be leaked and your property might be at risk. Here's what apps will be allowed to do:

- Influence the system's security and stability
Install apps that might contain viruses or misbehave in any other way
- Install dangerous apps
Some third party apps might attack your device, putting your data and privacy at risk

I'm aware of the possible risks, and assume all possible consequences voluntarily.

OK (7)

Cancel



Security error
zruloc.com



The site ahead contains dangerous apps

Attackers currently on **vznsrui.com** could install dangerous apps that damage your device, add hidden charges to your mobile bill, or steal your personal information. [Learn more](#)



To get Chrome's highest level of security, [turn on enhanced protection](#)

Back to safety

Details

File might be harmful

Do you want to download [redacted].apk anyway?

Cancel

Download anyway

هشدار امنیتی نصب برنامه نا ایمن



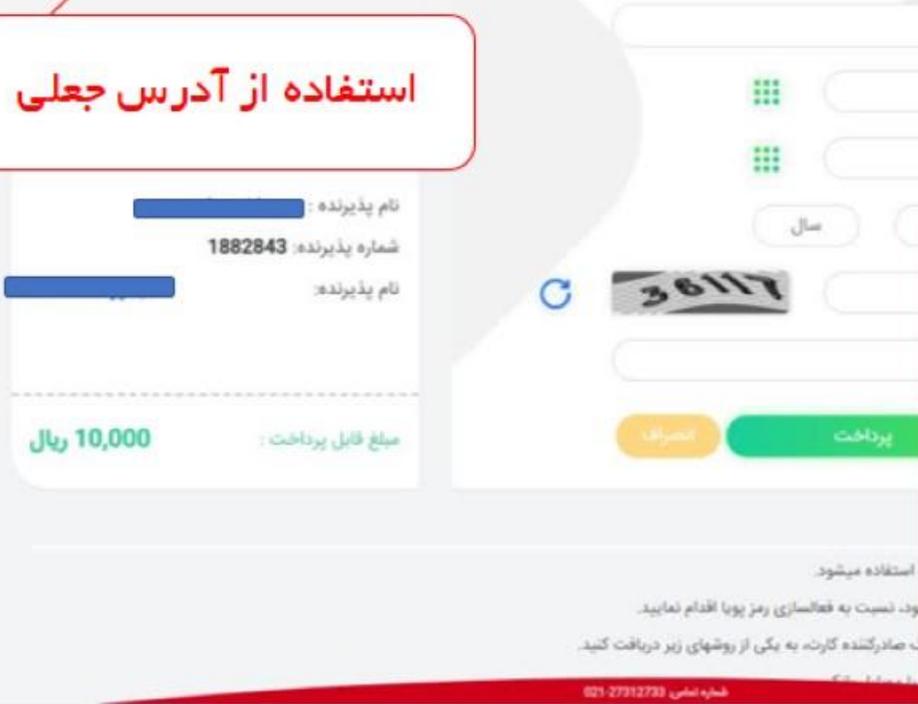
درگاه پرداخت جعلی

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 و تراکنش 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 خودداری فرمایید





پنج توصیه نجات بخش

پیامک های اطلاع رسانی مربوط به سازمان ها با سرشماره های اسمی ارسال می گردد.

1

هرگونه پیامک خدماتی از سرشماره های شخصی نامعتبر است.

2

به آدرس وب سایت ها، متن پیامک دریافتی و هشدارهای امنیتی مرورگر توجه کنید.

3

تمامی درگاه های بانکی به دامنه SHAPARAK.IR ختم می شوند.

4

در صورت دریافت پیامک مشکوک از طریق شماره ۰۹۶۳۸۰ با کارشناسان پلیس فتا مشورت کنید.

5

خروج از بحران

اطلاع رسانی به دیگران

گزارش به پلیس فتا

پیگیری قضایی

قطع اینترنت تلفن همراه

حذف برنامه جعلی

تخلیه حساب بانکی از خودپرداز

بِسْمِ
الرَّحْمَنِ
الرَّحِيمِ



کلاهبرداری در بسترسایت های ثبت آگهی

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





انواع کلاهبرداری در سایت های ثبت آگهی



دریافت بیعانه

۱

کلاهبرداری مثلثی

۲

رسیدساز جعلی

۳

کار در منزل

۴

جذب حمایت اجتماعی

۵





۱ - کلاهبرداری دریافت بیعانه



ثبت آگهی جعلی با
قیمت بسیار مناسب



دریافت بیعانه



خریدن زمان

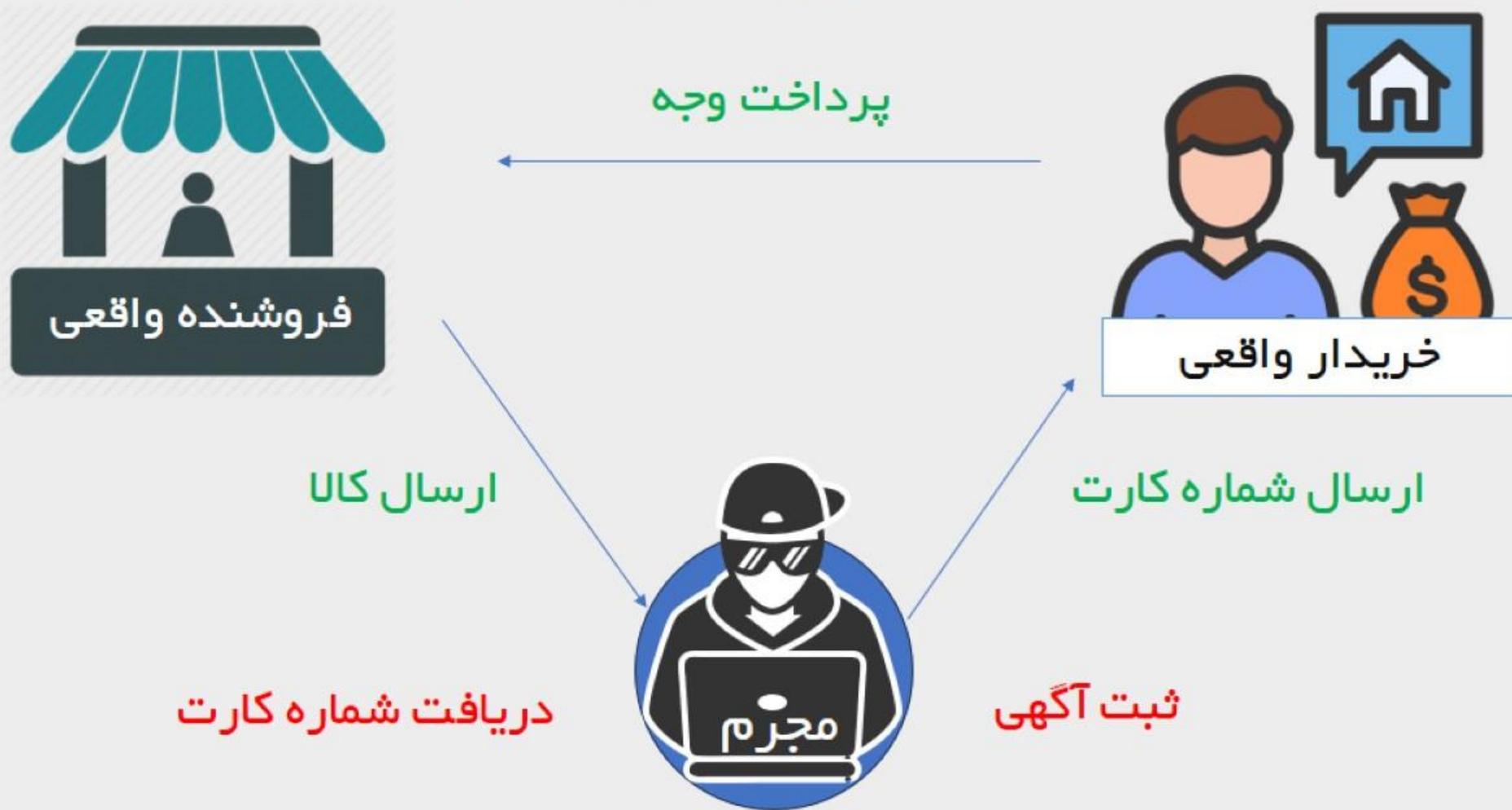


از دسترس
خارج شدن

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



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



۵- جذب حمایت اجتماعی

جذب
سرمایه

خیریه

مشارکت
شغلی

بیماران



ثبت آگهی با موضوعات جذب
حمایت اجتماعی توسط
کلاهبرداران اینترنتی



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

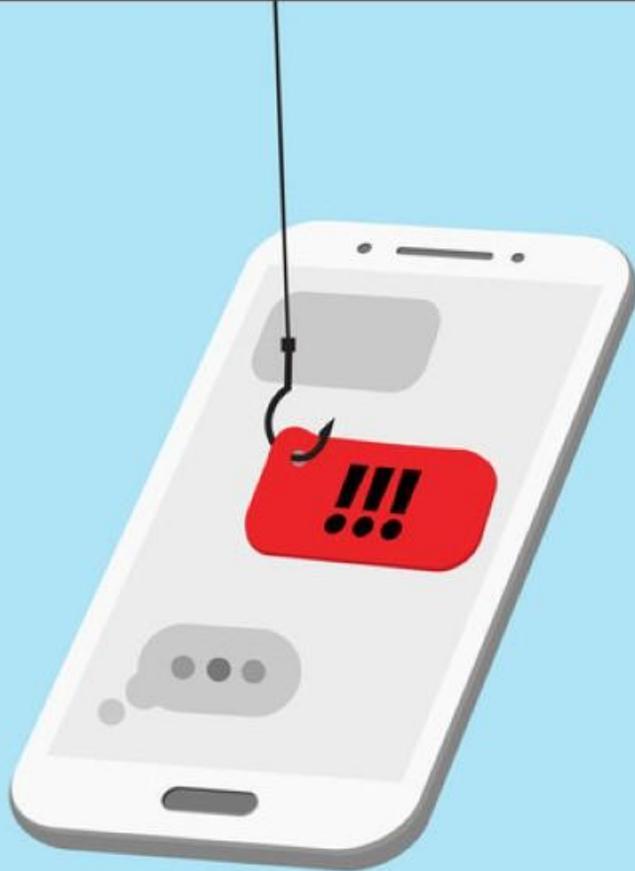
اسکیمر

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

بیمار نما ها

کمک های خود را از راه های مطمئن انجام دهید



پرداخت بیعانه

آگهی خودروی کرایه در سایت های ثبت آگهی

فروش وسایل سفر

برای کرایه خودرو
بین شهری بیعانه
پرداخت نکنید

به هیچ وجه بیعانه پرداخت نکنید



پلیس فضای تولید و تبادل اطلاعات

در هنگام راهپیمایی اربعین
برای درامان ماندن از خطر
اسکیمر
هنگام خرید از فروشندگان سیار
رمز را خودتان وارد کنید

اسکیمر

دست فروشان بین راهی

فروشندگان دوره گرد

فروشندگان غیر مجاز ارز

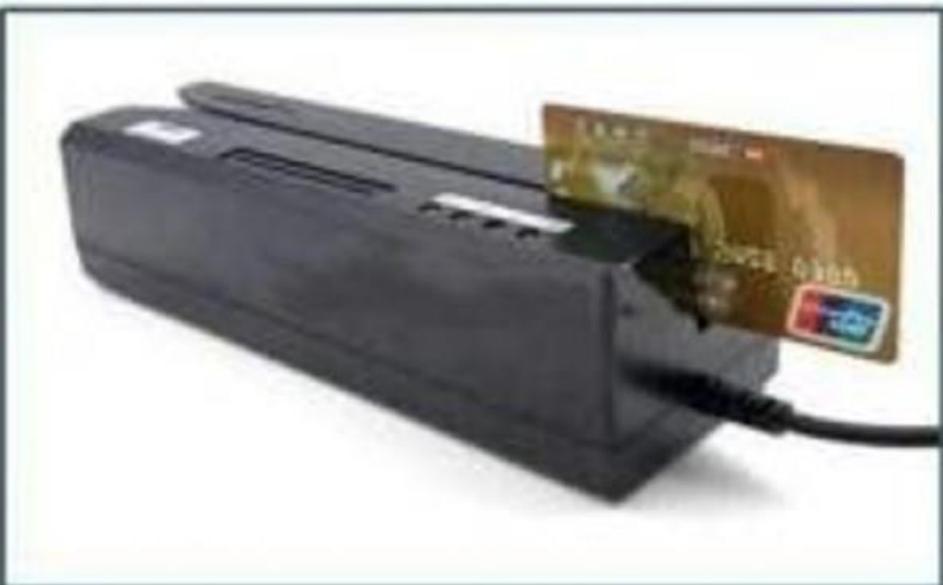
به سلامت کارت خوان توجه کنید

رمز کارت را خودتان وارد کنید

کارت پرداخت خرد داشته باشید



اسکیمر یک دستگاه کارتخوان غیرمجاز است که کلاهبرداران با استفاده از آن اطلاعات کارت شما را کپی می



اسکیمر

credit card
skimming
device



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

تشخیص کارتخوان واقعی از جعلی

لینک های جعلی

خرید ارز اربعین

اینترنت رایگان اربعین

دریافت گذرنامه

برنده شدن در رادیو اربعین

به پیام های دریافتی از سر شماره های
شخصی با عناوینی همچون **ارز اربعین**،
اینترنت رایگان، **گذرنامه** و ... اعتماد
نگرده و به هیچ عنوان وارد **لینک های
جعلی** ارسالی نشوید

مرکز فوریت های سایبری
www.CyberPolice.ir

به هیچ وجه لینک های مشکوک **پیامک شده** و دریافت شده در
پیامرسان ها را باز نکنید



بهداشت امنیت سایبری

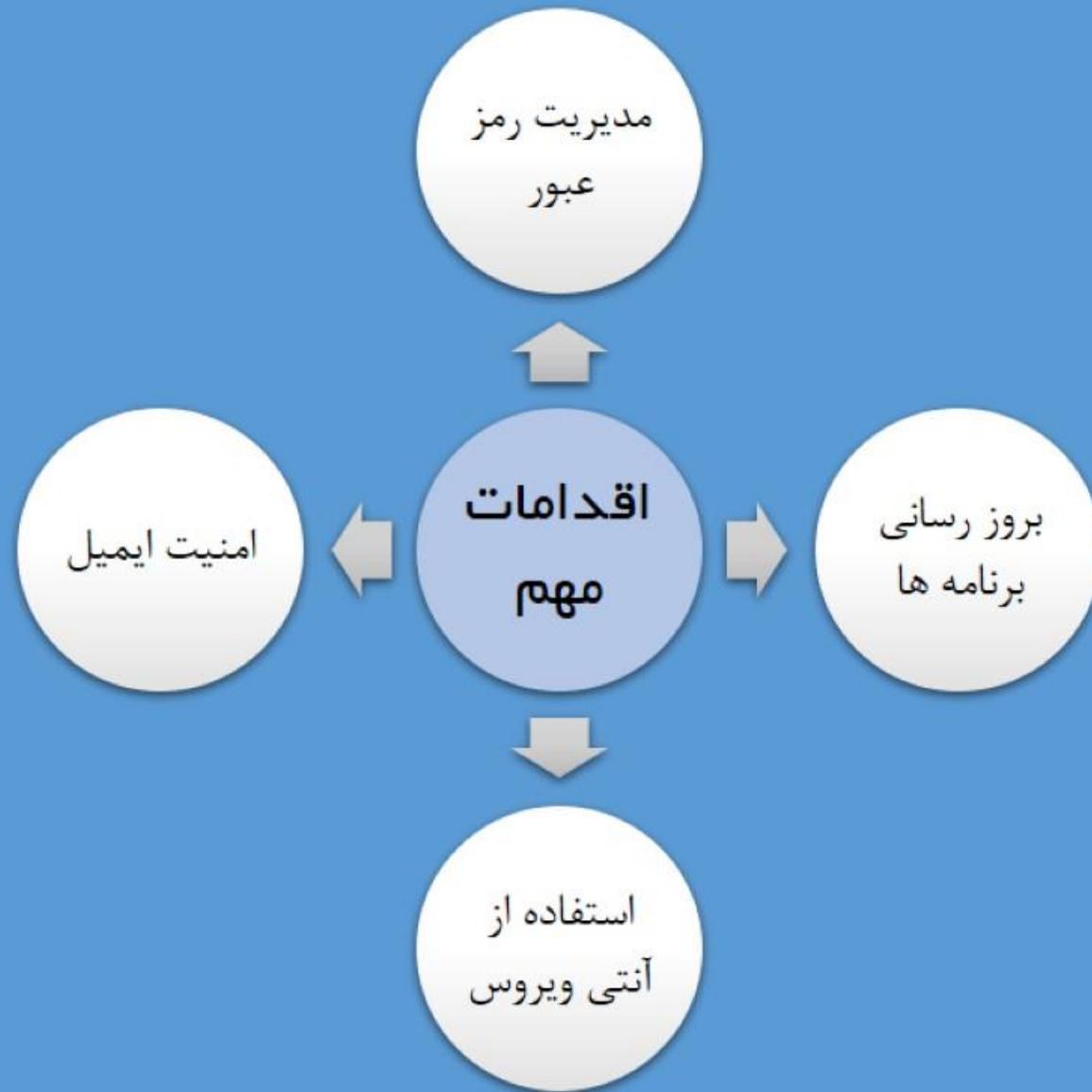
آشنایی با مجموعه راهکارهای حفظ سلامت و امنیت
کاربران، دستگاه‌ها، شبکه‌ها و داده‌ها





بهداشت امنیت سایبری چیست؟

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



اقدامات مهم برای امنیت سایبری

۱ - مدیریت رمز عبور

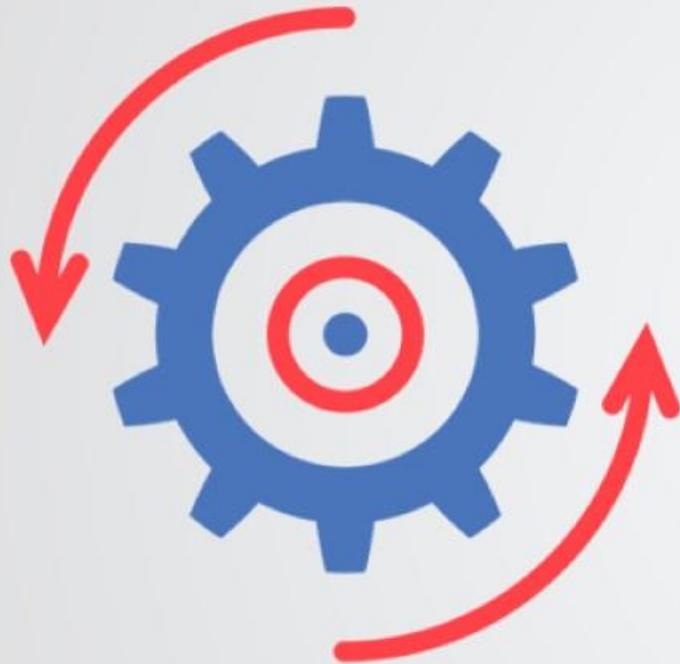


- ترکیب حروف بزرگ + حروف کوچک + عدد + نشانه
- طول ۱۴ کاراکتر یا بیشتر

اشتباهات رایج در امنیت رمز عبور



۲- به روز رسانی برنامه ها



Update...

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

جایگزینی نرم افزارهای
منسوخ یا پشتیبانی نشده

به روزرسانی ها از
منابع معتبر

تنظیم به روزرسانی ها
برای اجرای خودکار

۳- استفاده از آنتی ویروس



جویش کنید



به هشدارها توجه کنید



به روز نگاه دارید

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



Gmail



توصیه مهم

• حداقل سه ایمیل داشته باشید

• ایمیل برای وبگردی و کارهای متفرقه



• ایمیل برای راه اندازی شبکه های اجتماعی



• ایمیل برای امور شخصی





وارد Gmail شوید و
My Account را انتخاب

1

افزایش امنیت G-Mail

My Account

Sign-in & security >

Control your password and Google Account access.

- [Signing in to Google](#)
- [Device activity & security events](#)
- [Apps with account access](#)

انتخاب Signing in to Google

 Get your account in just a few minutes by reviewing your security and activity.

2

[GET STARTED](#)



Find your phone

Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet.

[GET STARTED](#)

Personal info & privacy >

Manage your visibility settings and the data we use to personalize your experience.

- [Your personal info](#)
- [Manage your Google activity](#)
- [Ads Settings](#)
- [Control your content](#)



Privacy Checkup

Take this quick checkup to review important privacy settings and adjust them to your preference

[GET STARTED](#)

Last checkup: March 14, 2016



My Activity

Discover and control the data that's created when you use Google services

Account preferences >

Adjust account settings, like payment methods, languages, & storage options.

- [Payments](#)
- [Language & Input Tools](#)
- [Accessibility](#)
- [Your Google Drive storage](#)
- [Delete your account or services](#)

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

The screenshot shows the 'Password & sign-in method' section of a Gmail account settings page. A yellow circle with the number '3' highlights the 'Password' row. Red arrows point from Persian text boxes to the '2-Step Verification', 'App passwords', and 'Recovery email' rows. The 'Recovery phone' row is partially visible at the bottom.

Password & sign-in method		
<p>Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if somebody manages to steal your password, it is not enough to get into your account.</p> <p>Note: To change these settings, you will need to confirm your password.</p>		
Password	Last changed: January 10, 2015	>
2-Step Verification	On since: Just now	>
App passwords	None	>
Account recovery options		
<p>If you forget your password or cannot access your account, we will use this information to help you get back in.</p>		
Recovery email	██████████@gmail.com	>
Recovery phone	██████████	>

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 کارتان 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

