
بسم الله الرحمن الرحیم

اینترنت

انگیزه بزهکاران سایبری از قربانی قرار دادن کاربران

بزرگ‌ترین سامانه ای است که تاکنون به دست انسان طرّاحی، مهندسی و اجرا شده است.

اینترنت یک شبکه جهانی توزیع شده‌است که شبکه‌های خودمختار به انتخاب خود به آن پیوسته‌اند و بدون هیچ بدنه مرکزی فرماندهی کار می‌کنند.

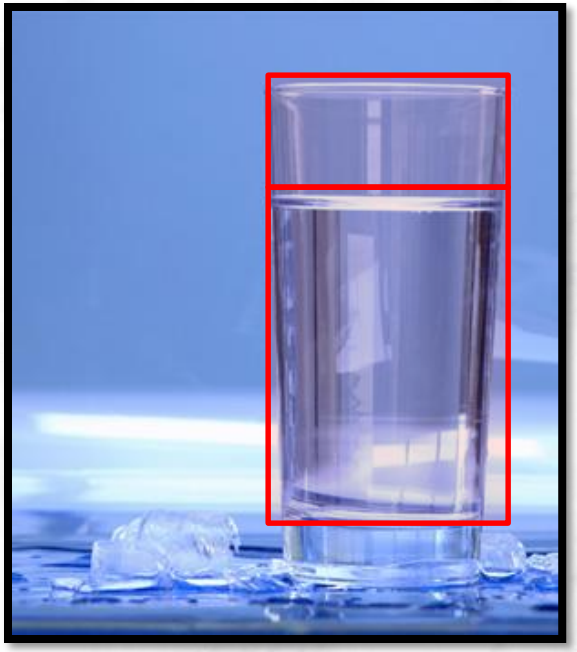
ویژگیهای اینترنت

- انعطاف پذیر و کارکرد عمومی
- فارغ از زمان و سریع
- فارغ از مکان و جغرافیا
- در دسترس بودن برای عموم
- مقرون به صرفه بودن

کارکردهای اینترنت

- منبعی عظیم از مطالب علمی
- بستری رایگان برای تجارت
- ابزاری کارآمد برای مبادله و اشتراک گذاری اطلاعات
- کم کردن فاصله ها و تسهیل ارتباطات اجتماعی
- ابزاری برای سرگرمی و تفریح
- ایجاد بستری راحت برای انجام کارهای مشارکتی
- ایجاد امکان دسترسی از راه دور به رایانه‌های دیگر
- قابلیت انتشار محتوای ترکیبی(عکس،فیلم، متن، صدا و...)

لزوم یا عدم لزوم استفاده اینترنت



با این همه مزایا و قابلیت های بی نظیر اینترنت بی شک در اولین نگاه، نیمه پر لیوان تاثیرات استفاده از اینترنت در جامعه، خود نمایی می کند.

اما این به هیچ عنوان به این معنی نیست که از نیمه خالی لیوان که گاهاً خانمان سوز است چشم بپوشیم.

با نیمه خالی لیوان چکار کنیم؟

۱- فرهنگ استفاده درست را ترویج دهیم

۲- دانش استفاده از این تکنولوژی را فرا بگیریم

انگیزه بزهکاران سایبری

Menu

انگیزه بزهکاران سایبری از قربانی قرار دادن کاربران

- ورود به حریم خصوصی افراد برای اخاذی های جنسی
- ورود به حریم خصوصی افراد برای اخاذی های مالی
- هتک حیثیت افراد برای آزار و اذیت و انتقام جویی
- برقراری ارتباط با افراد به منظور اغفال و برقراری روابط ناسالم
- کلاهبرداری های مالی
- مردم آزاری
- کنجکاوی و محک زدن توانایی های علمی

تلفن همراه
و حافظه های جانبی

تلفن همراه و حافظه های جانبی

امکانات،تجهیزات و اطلاعات گوشی

- پیامک
- دفترچه تلفن
- میکروفون
- برقراری تماس
- دوربین
- فایل های تصویری
- فایل های صوتی
- عکس
- نرم افزار ها و اطلاعات بانکی
- حافظه های جانبی

حریم خصوصی تلفن های همراه

امکانات،تجهیزات و اطلاعات گوشی

حریم خصوصی

- پیامک
- دفترچه تلفن
- میکروفون
- برقراری تماس

آلبوم کامل خانوادگی که درگذشته جای آن گنجه خانه بود

- دوربین
- فایل های تصویری
- فایل های صوتی
- عکس

اطلاعات مالی که در گذشته در گاوصندوق ها نگهداری می شد

- نرم افزار ها و اطلاعات بانکی
- حافظه های جانبی

حریم خصوصی تلفن های همراه

امکانات،تجهیزات و اطلاعات گوشی

آلبوم خانوادگی | حریم خصوصی | اطلاعات مالی

ممکن است:

جا بماند یا کم شود | به سرقت برود | هک شود

با سهل انگاری در اختیار افراد غیر مجاز قرار گیرد

و یا اطلاعات پاک شده آن توسط بزهکاران بازیابی شود

سرقت اطلاعات خصوصی از طریق حافظه های جانبی

❖ بنا بر این بخاطر داشته باشید ...

۱- حافظه های جانبی مانند فلش مموری و ... به دلیل جابجایی های مکرر به هیچ عنوان رسانه ی امنی برای حفظ اطلاعات حساس نیستند.

۲- داده های دیجیتال خود را روی رسانه هایی مانند سی.دی یا دی.وی.دی ذخیره کنید و آنها را در محلی امن و مورد اطمینان نگهداری کنید.

۳- هیچگاه رسانه های ذخیره سازی شخصی را دراختیار افراد ناشناس قرار ندهید.

۴- برای تمامی حافظه های جانبی خود (در صورت امکان) ،کلمه عبور مناسب تعریف کنید.

۵- حتی اطلاعات غیر حساس را به صورت طولانی مدت در حافظه های جانبی نگه داری نکنید و به محض اتمام کار، اطلاعات خود را از این حافظه ها پاک کنید.

رمز عبور

انتخاب رمز عبور مناسب برای تجهیزات و سامانه های رایانه ای

- تمامی سامانه ها و تجهیزات رایانه ای باید دارای کلمه عبور مناسب باشد.
- به خاطر داشته باشید کلمات عبور نا مناسب براحتی برای بزهکاران قابل حدس خواهد بود.

یک کلمه عبور مناسب باید:

- ✓ غیر قابل حدس زدن باشد
- ✓ بلند باشد
- ✓ ترکیبی از حروف، اعداد و علائم باشد
- ✓ بین چند دستگاه یا سامانه مشترک نبوده و منحصر به همان سامانه یا دستگاه باشد
- ✓ مدت زمان طولانی استفاده نشود و در فواصل زمانی مناسب تغییر کرده باشد.

بدافزار

Menu

بدافزارها

بد افزار چیست؟

ویروس، تروجان، کرم و تمامی برنامه های کامپیوتری است که فعالیتی را بـدون آگاهی، اجازه و خواست شما بر روی کامپیوترتان انجام می دهند.

بد افزار ها از چه طریق وارد سیستم ما می شوند؟

- حافظه های جانبی آلوده به ویروس
- دانلود فایل های آلوده به ویروس
- دریافت ایمیل های آلوده
- دریافت فایل های آلوده از طریق شبکه های بی سیم
- استفاده از فیلتر شکن ها

بدافزارها

راه کار مقابله با بد افزار ها

عدم استفاده از فیلتر شکن و VPN: فیلتر شکن ها به ارائـه دهنـده سـرویس فیلتـر شـکن، امکـان دسترسی به اطلاعات سیستم شما را خواهد داد. به هیچ عنوان بر روی سیستم هـا خـانگی از فیلتـر شکن استفاده نکنید.

کودکان

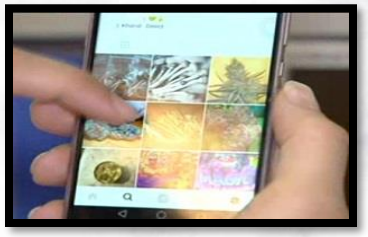
Menu

کودکان

❖ انگیزه بزهکاران برای برقراری ارتباط با کودکان و اعضای خانواده در فضای مجازی

۱- برقراری ارتباط و فریب کودکان در فضای مجازی، بمنظور کسب اطلاعات خانوادگی

۲- برقراری ارتباط با کودکان در فضای مجازی به منظور آزار و اذیت و سوء استفاده های جنسی مجازی



۳- برقراری ارتباط و فریب اعضای خانواده در فضای مجازی، به منظور برقراری ملاقات حضوری و روابط نا سالم

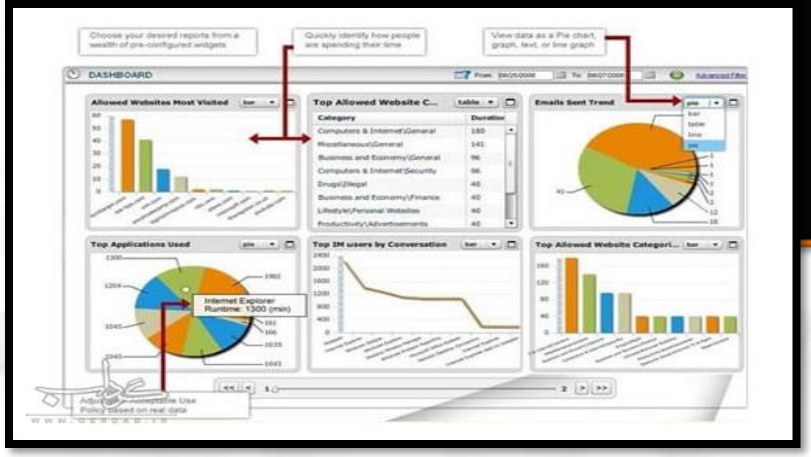
۴- فروش مواد مخدر در اینترنت که دامن گیر نوجوانان و جوانان، اعم از دختران و پسران شده است.

۵- تاثیرگذاری بر اعقادات و طرز تفکر کودکان درباره باورهای مذهبی و سیاسی

❖ بنا بر این به خاطر داشته باشید...

همواره بر فعالیت و ارتباطات اعضای خانواده خود به ویژه فرزندانتان در فضای مجازی نظارت درست و هوشمندانه داشته باشید و از ابزار های کمکی والدین در اینباره استفاده کنید.

نرم افزارهای کمکی والدین



نرم افزارهای کمکی والدین

نرم‌افزارهای کنترل‌کننده و محدودکننده به والدین کمک می‌کند تا هم بر فرزندان‌شان نظارت داشته باشند و هم اینکه گزارش فعالیت‌های فرزندشان را دریافت کنند.

این نرم افزارها در موارد زیر به والدین کمک می کنند:

۱- کنترل و نظارت کامل بر تماس‌های ورودی و خروجی

۲- کنترل و نظارت کامل بر پیامک‌های تلفن همراه فرزندان

۳- انتقال اطلاعات از طریق پست الکترونیکی

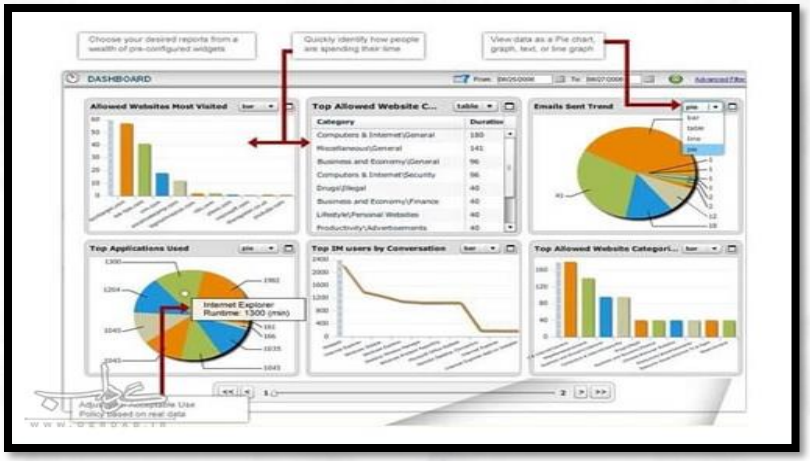
۴- کنترل و نظارت زمانی و اجرایی بر نرم‌افزارهای نصب‌شده و نرم افزارهایی که فرزندان می خواهند بر روی تلفن همراه خود نصب کنند.

۵- کنترل بر روی ساعات کار گوشی و کنترل موقعیت مکانی تلفن همراه فرزند

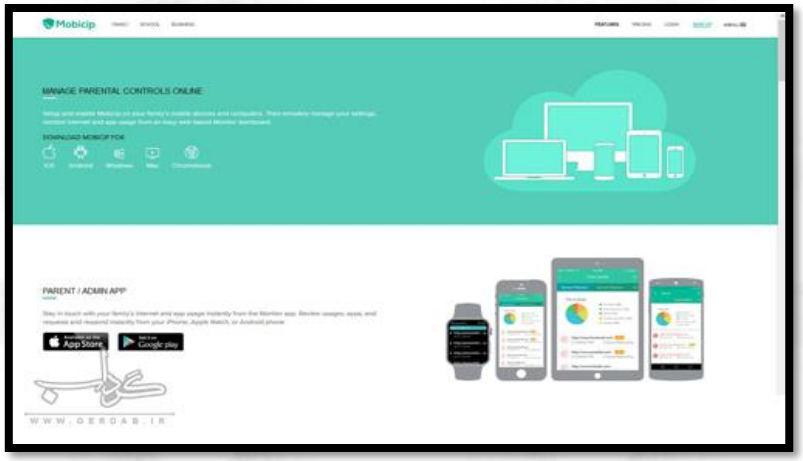
۶- کنترل مرورگر اینترنت

نرم افزارهای کمکی والدین

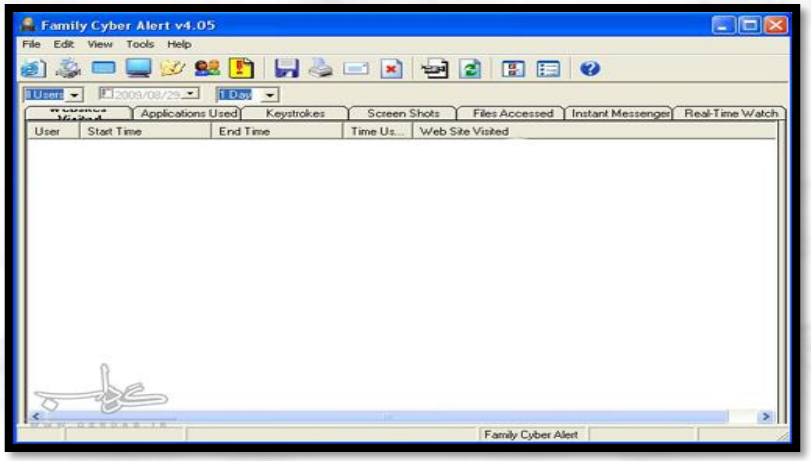
نمونه هایی از نرم افزارهای کنترل والدین



web watcher



mobicip



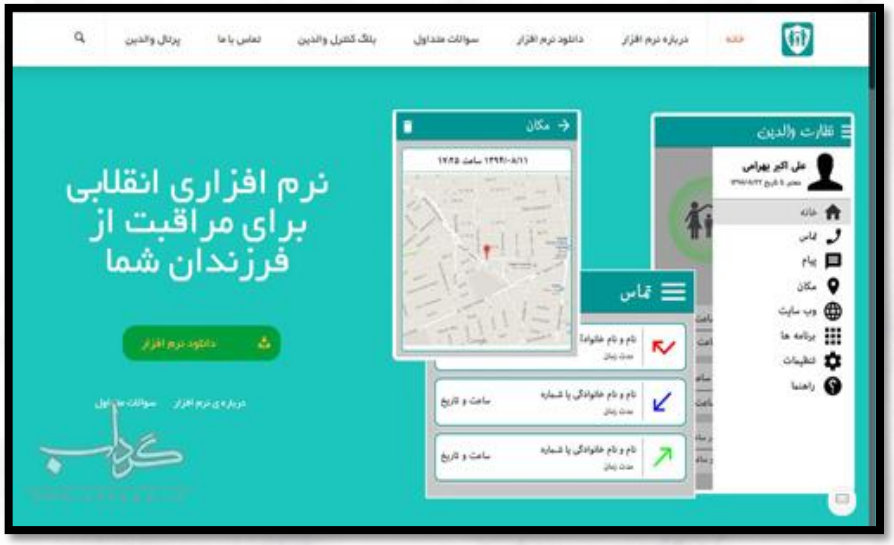
Family Cyber Alert

Hidetools Parental Control

نرم افزارهای کمکی والدین

نمونه هایی از نرم افزارهای کنترل والدین

سامانه مراقبت از خانواده در دنیای مجازی (Spf)



نرم‌افزار کنترل والدین سانیار۸

Menu

شبکه های اجتماعی

Menu

شبکه های اجتماعی

شبکه اجتماعی ساختاری اجتماعی است که از افرادی که توسط یک یا چند نوع خاص از وابستگی مانند ایده‌ها و تبادلات مالی، دوستان، خویشاوندان و ... هم وصل هستند.

بر اساس قانون جرایم رایانه‌ای اصل بر آزادی است و شهروندان از تمامی امکانات اینترنت می‌توانند استفاده کنند اما این اصل استثناهایی دارد که عمدتاً در قانون جرایم رایانه‌ای آمده است.

پیش از اشاعه و ترویج هر امکاناتی در هر جامعه نیاز است تا فرهنگ استفاده از آن ذکر شود. چه بسا امکانات و وسایلی که جهت رفاه در جامعه بودند اما با فقدان فرهنگ استفاده از آن مضراتش بیشتر از منفعتش شده است.

آنچه که امروزه در شبکه های اجتماعی رخ می دهد، نداشتن فرهنگ و علم استفاده از این فضاست.

انتشار تصاویر و فیلم‌های خصوصی :

در فضایی مانند محیط اینستاگرام افرادی هستند که با سوء استفاده از سادگی بعضی کاربران، تصاویر و فیلم های خصوصی آن ها را در فضای این نرم افزار انتشار می دهند.

هک اکانت:

در این فضا(اینستاگرام) هکرهای هستند که با هک کردن حساب اینستاگرامی کاربران آن را بدست می گیرند و در قبال برگرداندن حساب اینستاگرام و منشتر نکردن اطلاعات و تصاویر شخصی کاربران از آن ها پیشنهاد های مانند دریافت پول و... دارند.

توهین و فحاشی :

بسیار دیده می شود که صفحه اینستاگرام بازیگران ،هنرمندان، فوتبالیست ها و ... مورد توهین و فحاشی بسیاری از کاربران قرار می گیرد و شاهد واکنش هایی از طرف اشخاصی که مورد اهانت قرار گرفته بودیم مانند بستن صفحه اینستاگرام خود ، حذف کردن صفحه و... .

طبق ماده ۶۰۸ قانون مجازات اسلامی :

«توهین به افراد، از قبیل فحاشی و استعمال الفاظ رکیک، چنانچه موجب حد قذف نباشد، به مجازات شلاق تا ۷۴ ضربه و یا ۵۰ هزار تا یک میلیون ریال جزای نقدی محکوم خواهد بود.» باید توجه داشت که توهین فقط از طریق لفظ نیست، توهین می تواند مشتمل بر نوشته کاغذی یا نوشته مجازی از قبیل پیامک، پیام های شبکه ای یا نوشته های صفحات اینترنتی باشد.

مهندسی اجتماعی

Menu

مهندسی اجتماعی

مهندسی اجتماعی چیست؟

مهندسی اجتماعی، سوء استفاده زیرکانه از تمایل طبیعی افراد به اعتماد کردن است.

مزایای مهندسی اجتماعی برای بزهکاران:

- ✓ نیاز به هیچ تخصص علمی ندارد.
- ✓ اطلاعات مهم و حساس توسط خود قربانی به فرد کلاهبردار داده می شود.
- ✓ قوی ترین سیستم ها و نرم افزار های امنیتی دنیا زمانی که خود کاربر فریب خورده باشد کارآیی نخواهند داشت.

نمونه هایی از ابزارهای مهندسی اجتماعی:

۱- سوء استفاده از احساسات زنان برای برقراری روابط عاشقانه به قصد برقراری روابط نا سالم، کسب تصاویر خصوصی و در ادامه اخاذی و باج خواهی از آنها

۲- فریب افراد به منظور کسب اطلاعات بانکی و مالی افراد

۳- فریب افراد به منظور هک کردن اکانت افراد در شبکه های اجتماعی

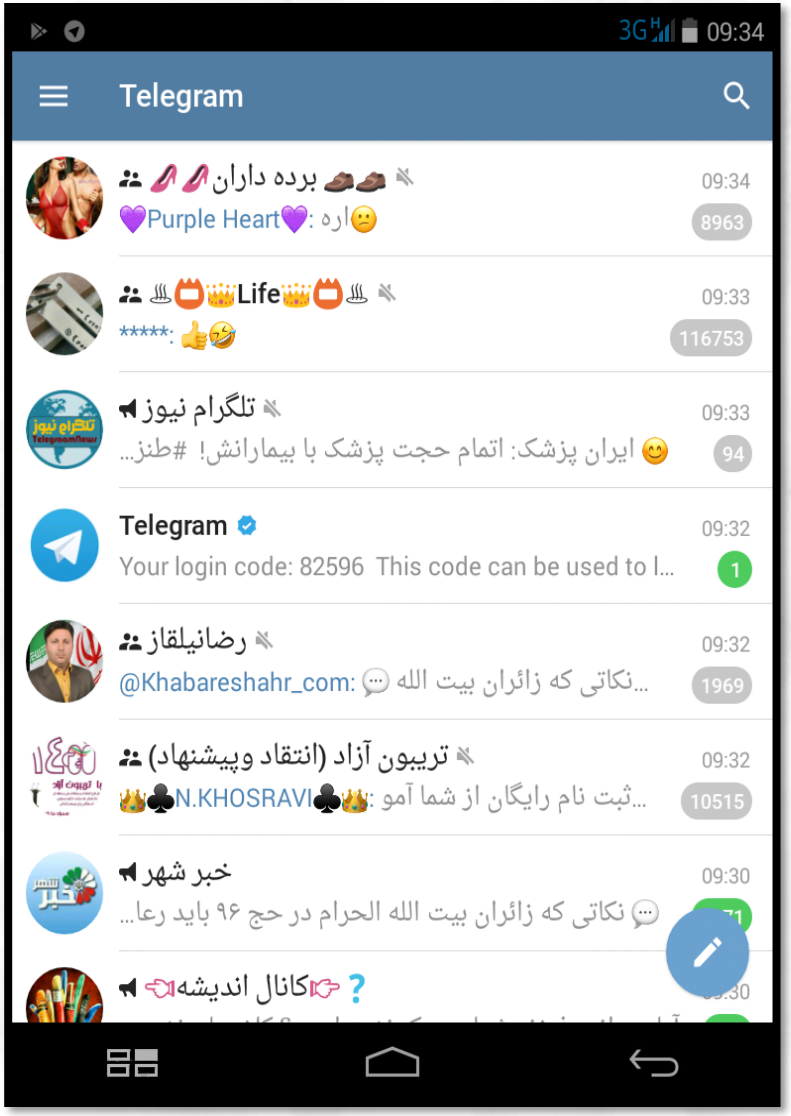
مهندسی اجتماعی

شبکه های اجتماعی برای برقراری امنیت خود از پروتکل های امنیتی بسیار قدرتمند استفاده می کنند که امکان هک کردن آنها تقریبا برای افراد حرفه ای نیز غیر ممکن است.

پس اکانت کاربران شبکه های اجتماعی چگونه هک می شود؟

- ✓ برای درک بهتر این موضوع یک سناریو واقعی را دنبال می کنیم...

مهندسی اجتماعی



شما اکانت تلگرامی را بر روی گوشی تلفن همراه خود نصب کرده اید

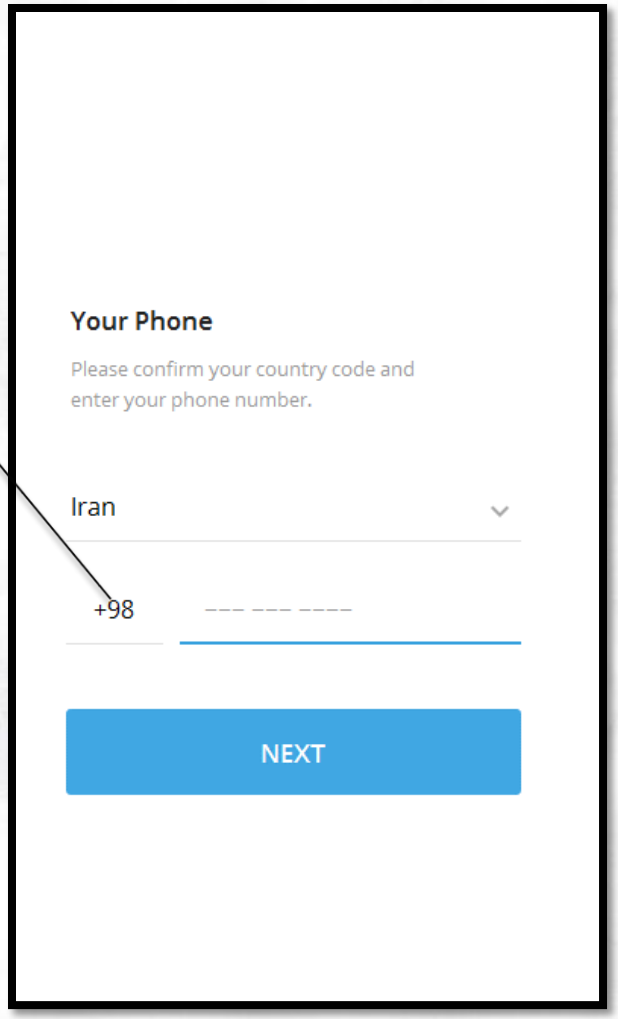
اگر شما بخواهید این تلگرام را به صورت همزمان بر روی رایانه خود نیز استفاده کنید، آیا این کار امکان پذیر است؟

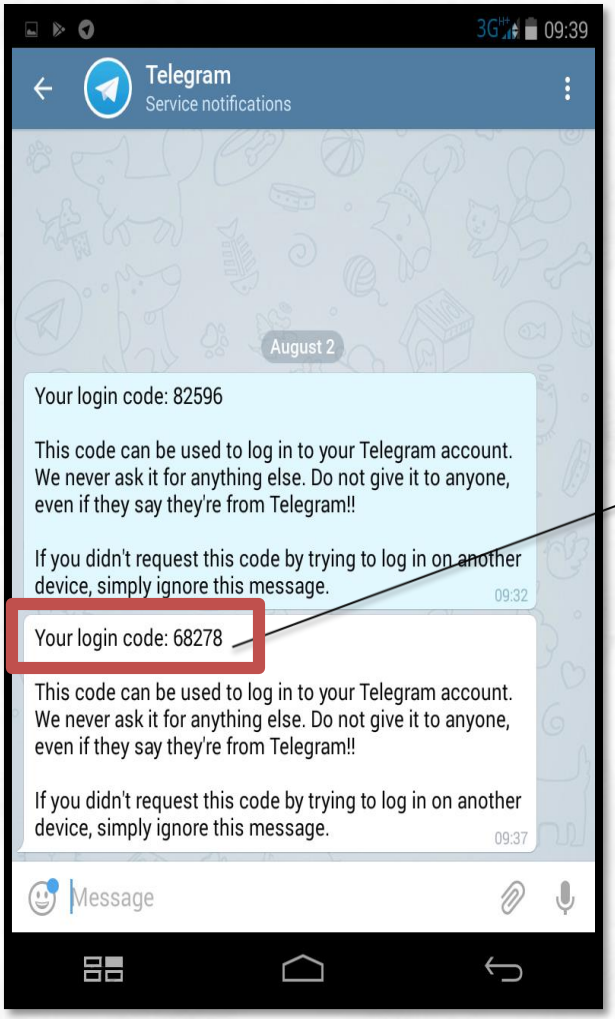
پاسخ مثبت است.
تلگرام این امکان را در اختیار شما قرار می دهد تا یک تلگرام را بر روی چند دستگاه استفاده کنید.

حال اگر دیگران بخواهند تلگرام شما را بدون اجازه شما بر روی دستگاه خودشان نصب کنند چه؟ آیا باز هم تلگرام اجازه نصب را خواهد داد؟

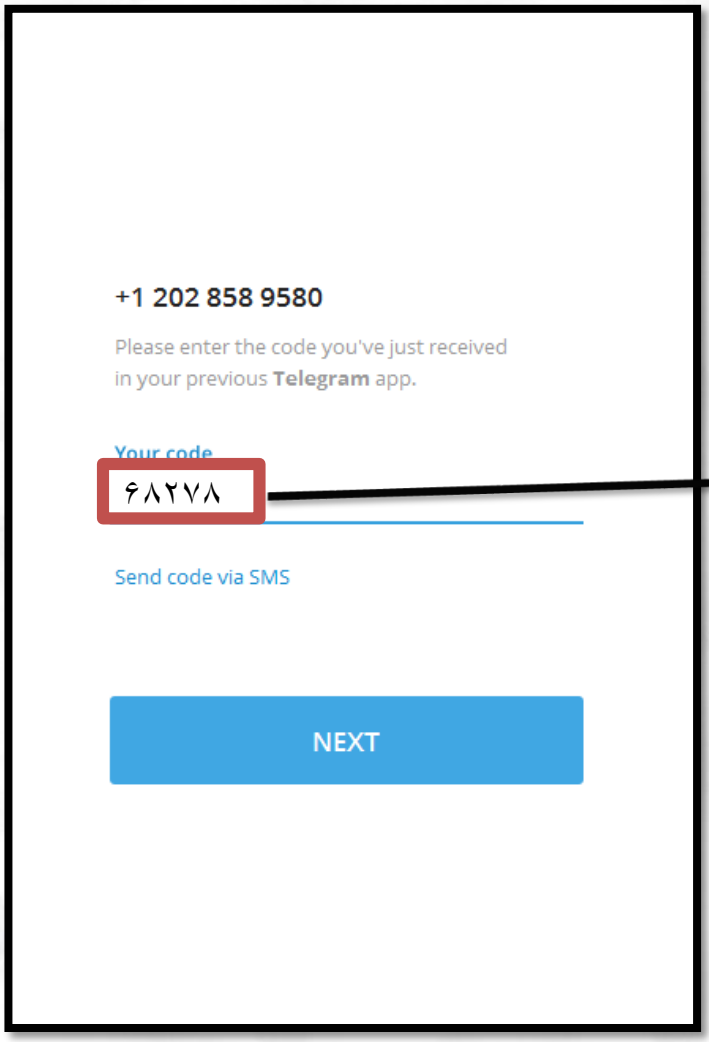
پاسخ منفی است.
تلگرام اجازه نصب تلگرام را بر روی دستگاهی دیگر می دهد، اما فقط دستگاه هایی که متعلق به خود شما باشد.

زمانی که شما شماره تلفن خود را در دستگاه جدید وارد می کنید تا از تلگرام خود بر روی آن دستگاه استفاده کنید، پیامی از سوی تلگرام به دستگاه فعلی شما ارسال می شود.





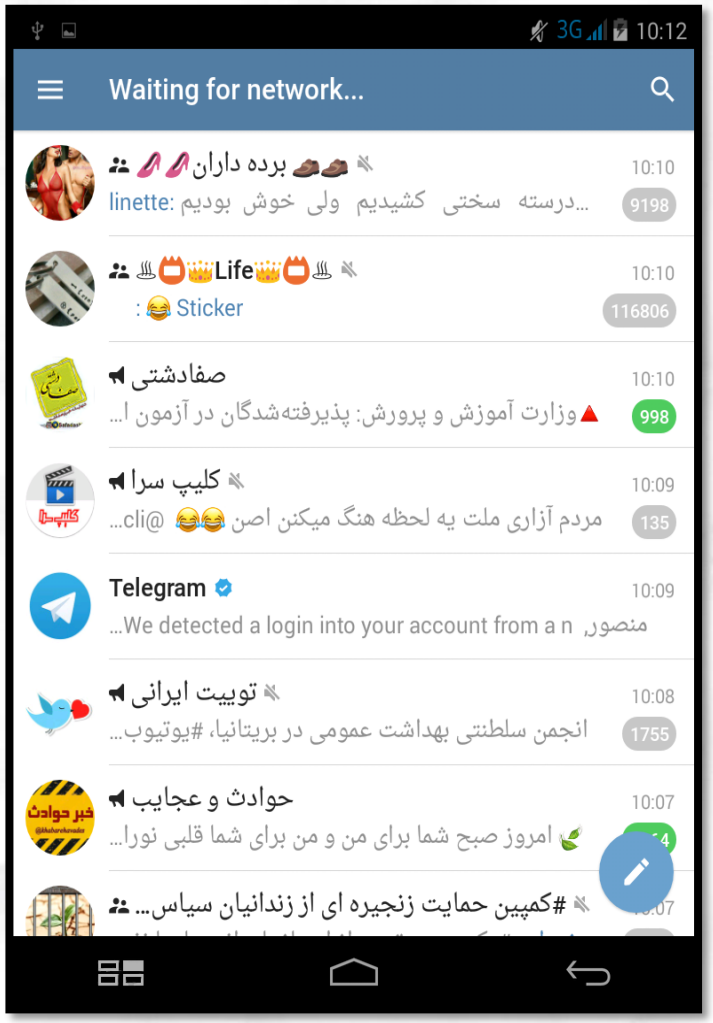
این همان پیغامی است که سوی تلگرام ارسال شده و به شما اعلام می کند این کد برای احراز هویت و ورود به اکانت تلگرام شما توسط دستگاهی دیگر است که نباید به هیچ عنوان در اختیار دیگران قرار گیرد.

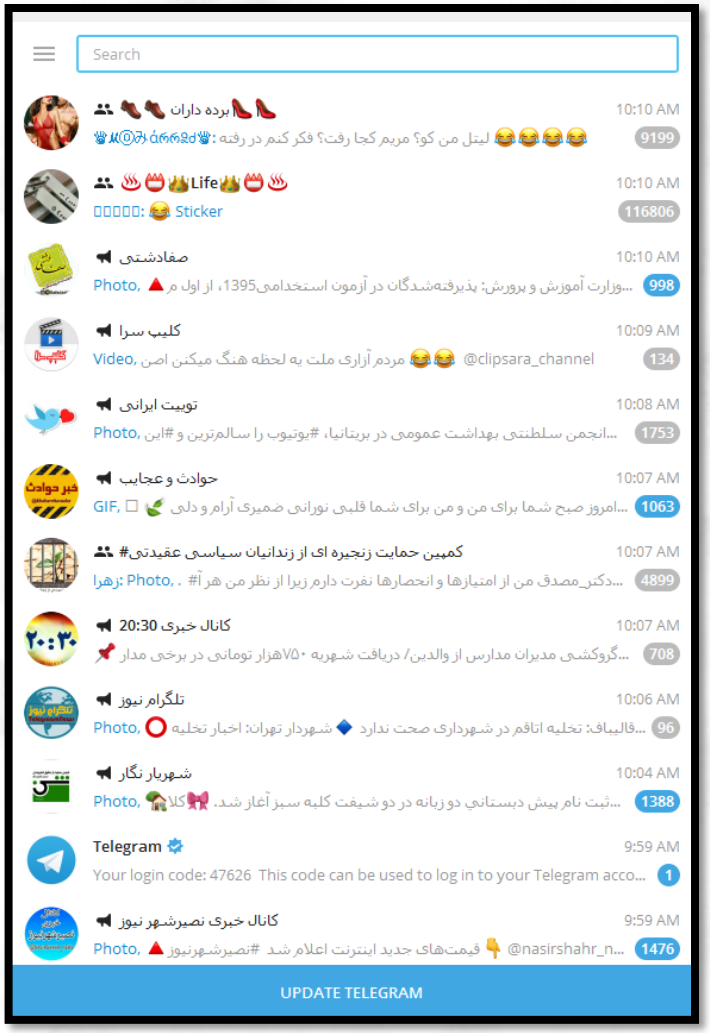


حال اگر کدی که از سوی تلگرام برای گوشی شما ارسال شده است را در دستگاه جدید وارد کنید، اکانت تلگرام شما بر روی هر دو دستگاه فعال خواهد بود

مهندسی اجتماعی

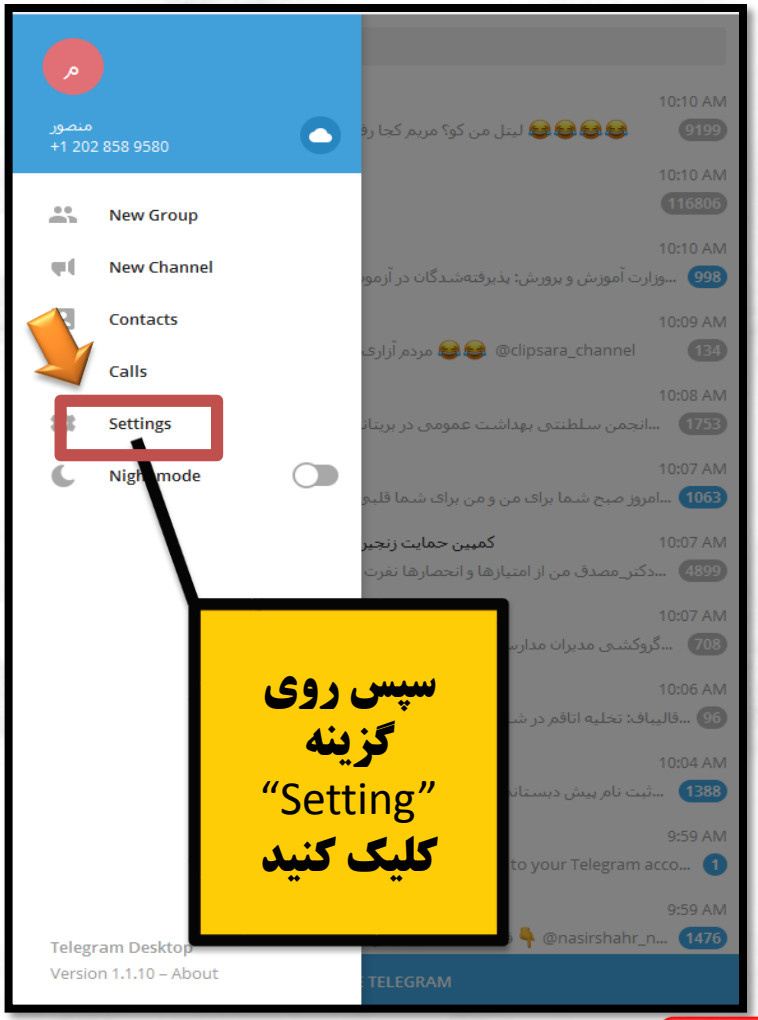
همانگونه که می بینید یک اکانت مشترک بر روی هر دو دستگاه فعال است.





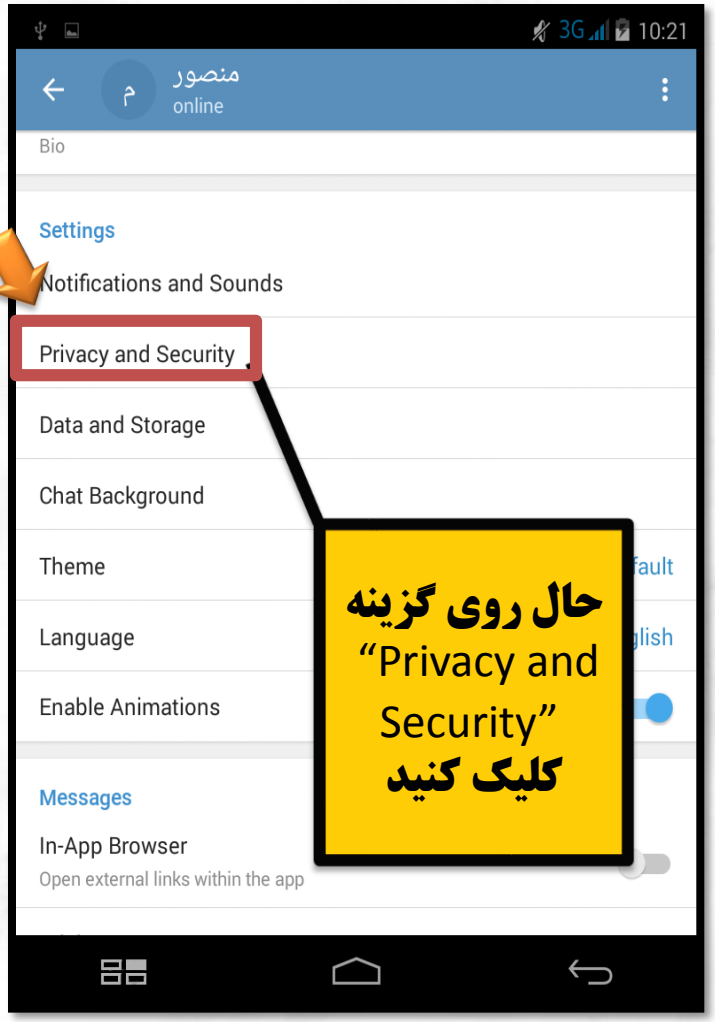
مهندسی اجتماعی

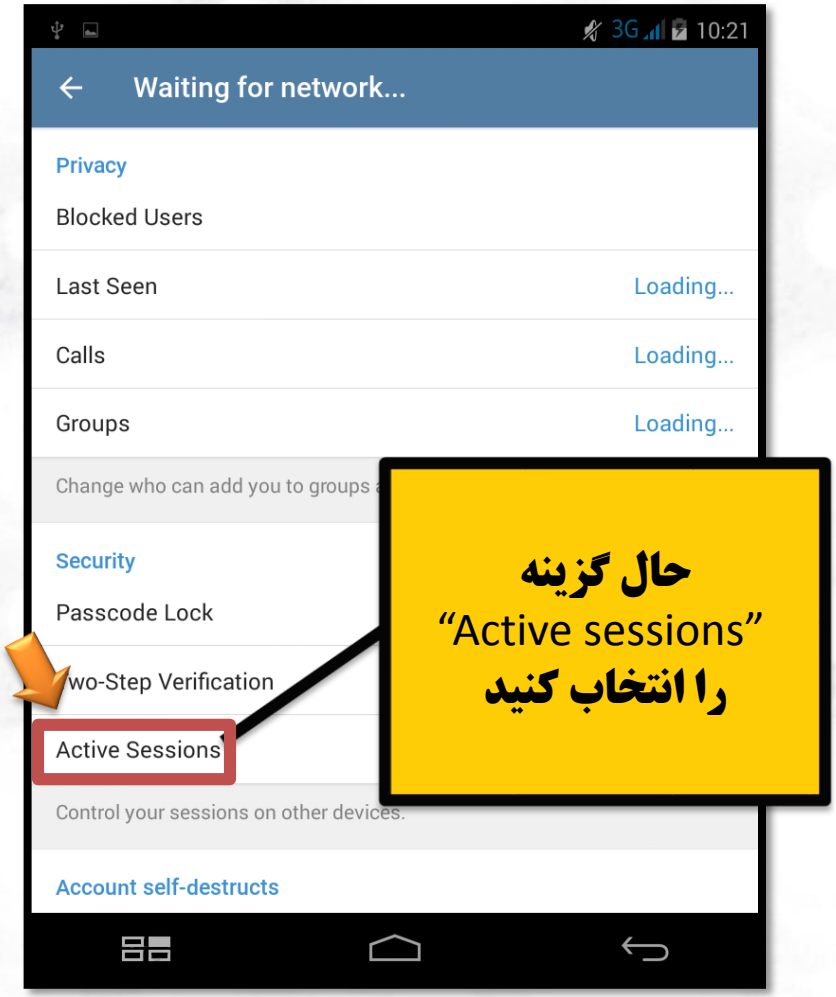
برای اینکه بدانید اکانت شما هم اکنون بر روی چه دستگاه هایی فعال است گام های زیر را طی کنید:



مهندسی اجتماعی

برای اینکه بدانید اکانت شما هم اکنون بر روی چه دستگاه هایی فعال است گام های زیر را طی کنید:





مهندسی اجتماعی

برای اینکه بدانید اکانت شما هم اکنون بر روی چه دستگاه هایی فعال است گام های زیر را طی کنید:

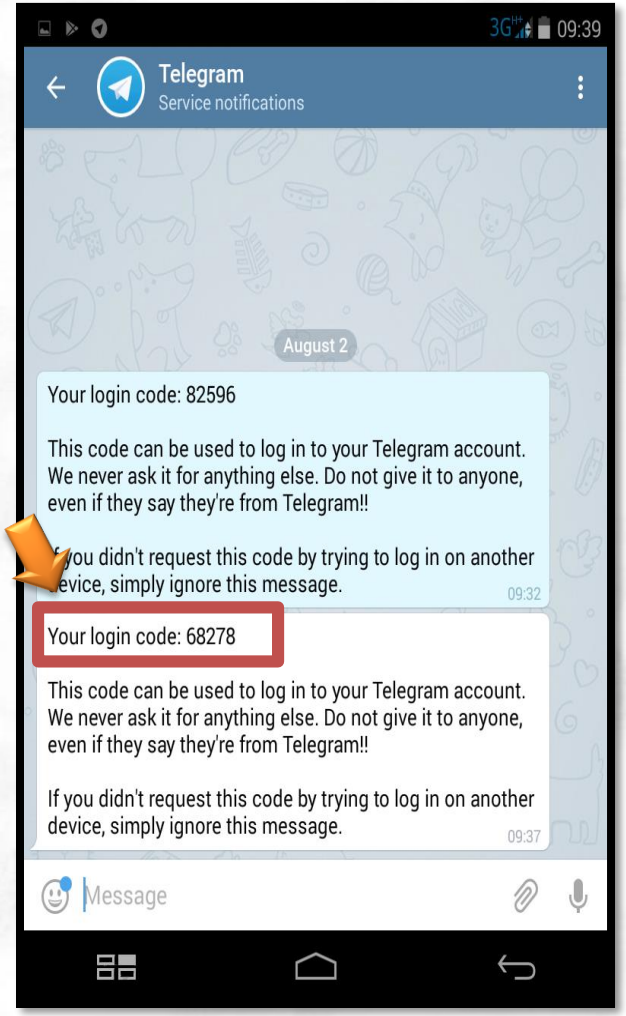
این قسمت مشخصات دستگاه فعلی شماست.

برای اینکه دسترسی سایر دستگاه های متصل به تلگرامتان را قطع کنید روی گزینه "Terminate ALL Other Sessions" کلیک کنید

این قسمت نشان دهنده سایر دستگاه هایی است که علاوه بر دستگاه خودتان در حال استفاده از تلگرام شما هستند

مهندسی اجتماعی

ترفند بزهکاران



بزهکاران شماره تلفن شما را در تلگرام وارد می کنند

تلگرام برای احراز هویت شما کدی رابرای شما ارسال می کند.

فرد بزهکار به هر طریق شما را فریب داده و کد را از شما می گیرد.

فرد بزهکار با وارد کردن کد در دستگاهش به تلگرام شما وصل شده و به تمامی اطلاعات خصوصی شما دسترسی می کند.

توجه!!!

هر کدی که از سوی شبکه های اجتماعی مانند تلگرام، فیس بوک، Gmail و ... برای شما ارسال می شود، به هیچ عنوان نباید در اختیار دیگران قرار بگیرد.

مهندسی اجتماعی

بنا بر این همواره به خاطر داشته باشید...

- ✓ به هیچ عنوان با افراد ناشناس در فضای مجازی ارتباط برقرار نکنید.
- ✓ به هیچ عنوان در فضای مجازی هویت واقعی خود را معرفی نکرده و به هویت اعلام شده توسط دیگران نیز اعتماد نکنید.
- ✓ مراقب روابط ناسالم و غیر اخلاقی در فضای مجازی باشید.
- ✓ احساسات و اعتماد، بهترین ابزار بزهکاران برای گرفتن اطلاعات از شما در فضای مجازی است.
- ✓ در صورت فعالیت در فضای مجازی و یا ارتکاب فعلی غیر مجاز در این فضا، هرگز از تهدید افراد به افشاگری نترسید و زمینه های ارتکاب اشتباهات بعدی را فراهم نکنید. و در اولین فرصت مراتب را به پلیس فتا اطلاع دهید تا از آسیب ها کاسته شود.

مهندسی اجتماعی

بنا بر این به خاطر داشته باشید...

- ✓ اگر اصرار به عضویت در شبکه های اجتماعی دارید، حتماً با ریز به ریز جزئیات امنیتی آنها آشنا باشید
- ✓ هرگز فراموش نکنید که بزهکارن سایبری با انگیزه های مختلفی دست به اعمال خرابکارانه می زنند. انگیزه هایی که شاید شما از آنها بی اطلاع باشید. پس با مصون دانستن خود، در حفاظت از اطلاعات خود سهل انگاری نکنید.
- ✓ در سامانه هایی که امکان تعریف رمز دوم(احراز هویت دو مرحله ای) دارد، این امکان را فعال کنید
- ✓ به خاطر داشته باشید در فضای مجازی «اطلاعات کم=امنیت بالا» است. بنابراین در سامانه ها و تجهیزات رایانه ای و همچنین شبکه های اجتماعی کمترین اطلاعات ممکن را ارائه داده و یا ذخیره نمایید.

چگونه از سرقت رفتن ایمیل خود جلوگیری کنید؟

www.cyberpolice.ir

فعال کردن اخطار از طریق پیامک برای حساب گوگل در صورت تغییر رمز و یا ورود مشکوک

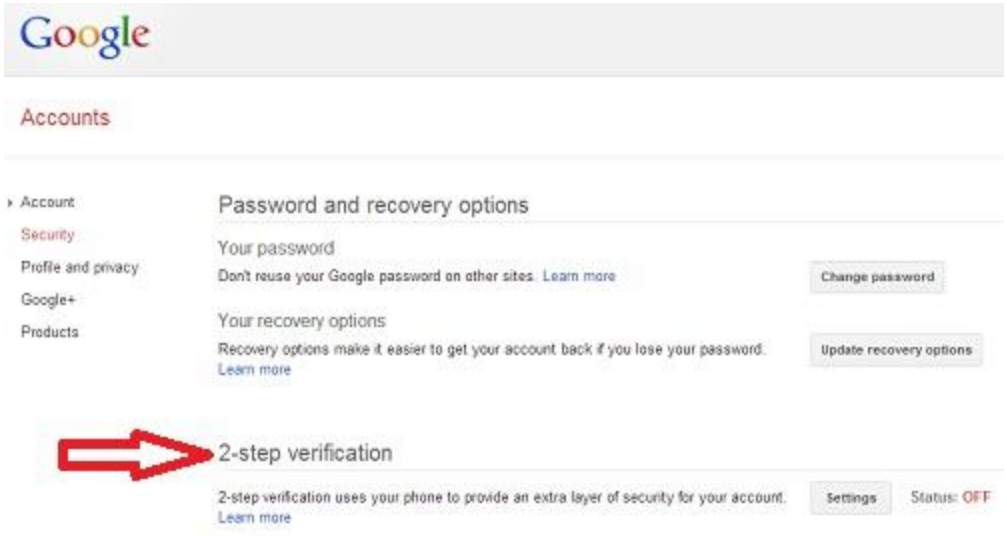
تاییدیه ۲ مرحله ای را فعال کنید

با فعال کردن این قابلیت گوگل هنگام **تغییر رمز** و یا **ورود مشکوک به حساب** یک پیام کوتاه برای شما ارسال می کند تا از وقوع هر گونه خسارتی جلوگیری کند.

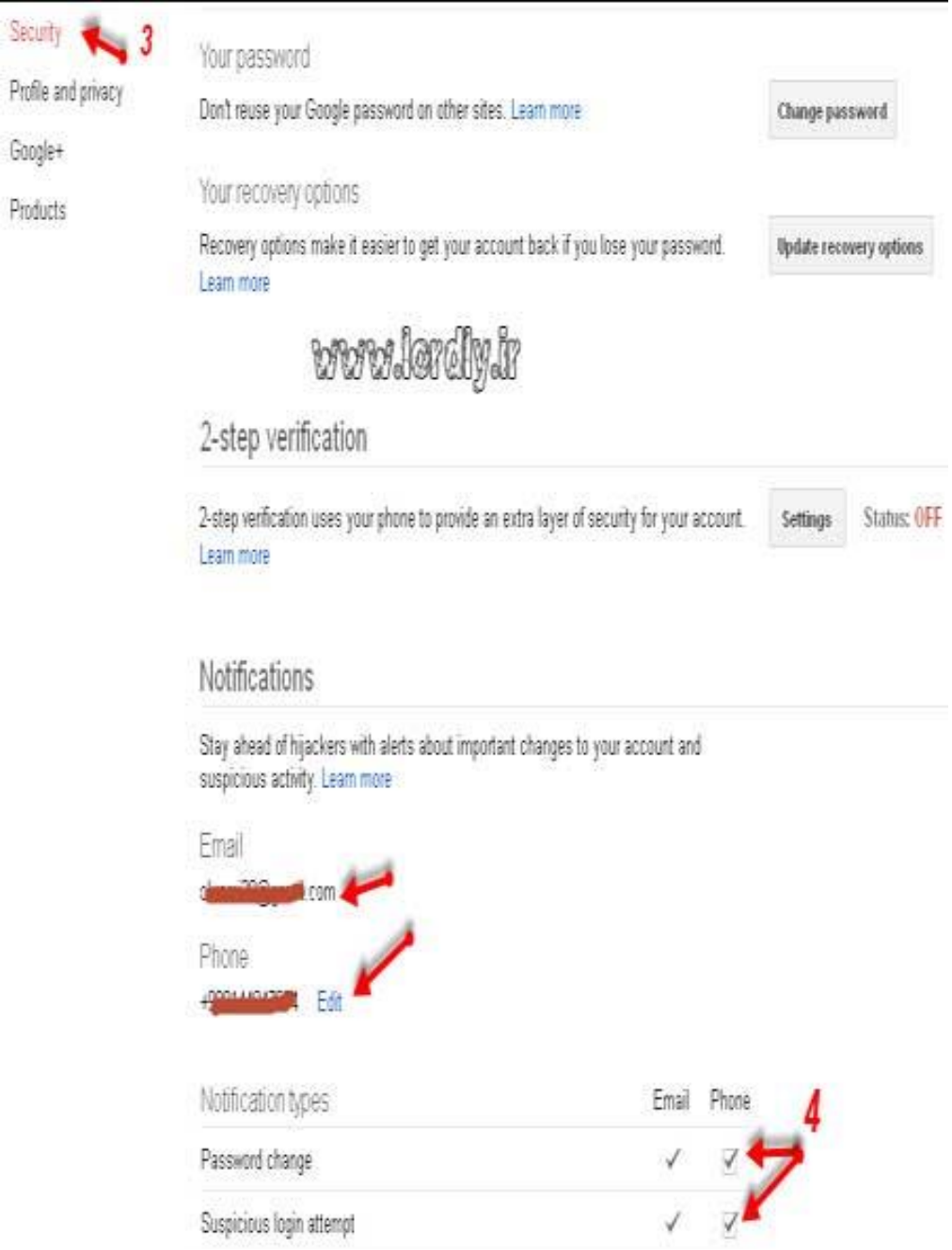
ممکن است شما آنلاین نباشید و از ایمیل خود خبری نداشته باشید با فعال کردن این عملکرد برای تلفن همراه شما همیشه و همه جا از حساب خود خبر دار هستید.

وقتی در حساب خود لاگین کردید. روی Account **کلیک کنید تا تنظیمات حساب کاربری نمایان شوند.**

>>از قسمت چپ گزینه ی Securiy **را انتخاب کنید.**



در این صفحه روی گزینه Settings **که در مقابل نوشته** step verification **است کلیک و در داخل صفحه جدید، شماره تلفن را وارد و این قابلیت را فعال کنید.**



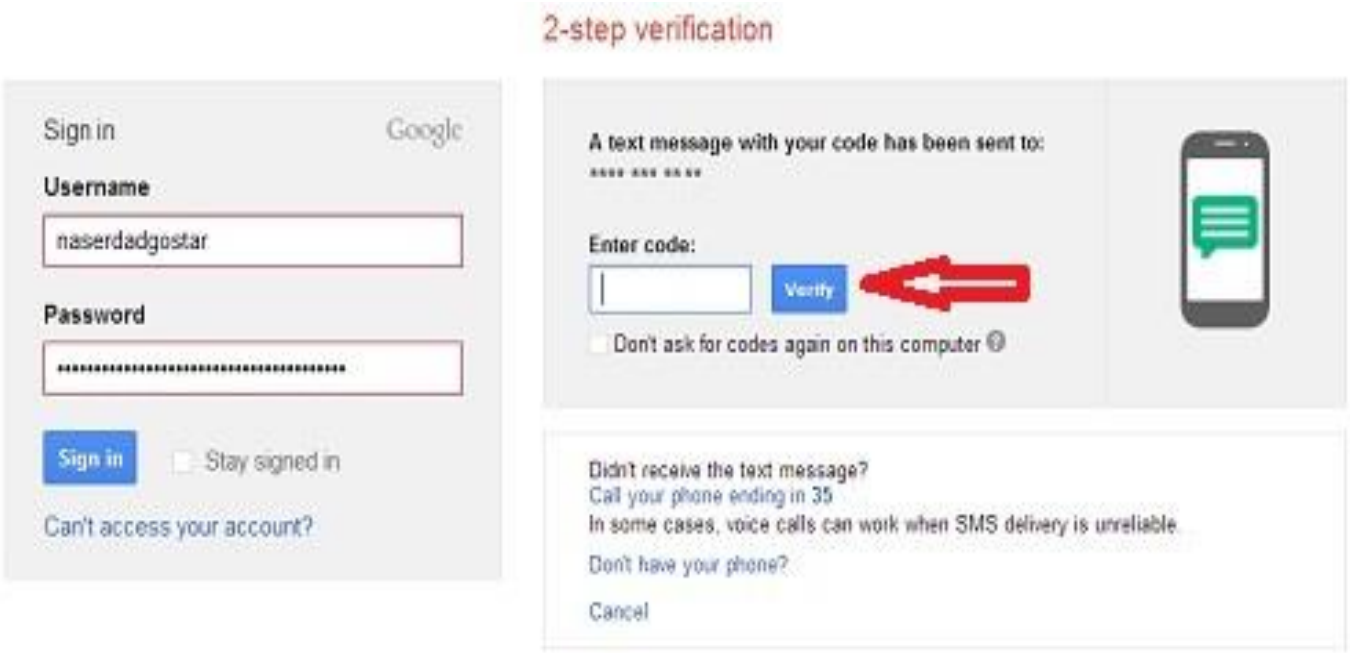
حالا به بخش Notification Types **رفته و تیک گزینه های** Phone **را بزنید.**

<<ردیف اول برای هشدار هنگام تغییر رمز است و ردیف دوم برای ورود های مشکوک. توجه:در این زمان برای شما کد امنیتی جدید ارسال خواهد شد

حالا شاید با خودتان بگویید اگر شماره تلفن من تغییر کرده باشد چه؟برای این کار در همین صفحه بر روی Edit جلوی شماره تلفن سابق خود کلیک کنید.

حالا از صفحه ی باز شده ابتدا کشور خود را انتخاب کنید
سپس شماره تلفن خود را بدون صفر اولیه وارد نمایید.بعد از این کار یک پیامک برای شما ارسال می شود که حاوی کد های امنیتی است،این کد ها را در قسمت Verify وارد نمایید و بر روی Verify کلیک کنید تا شماره تلفن جدید شما تایید شود.

وقتی این گزینه را فعال کردید، دسترسی به ایمیل تان همیشه نیازمند رمز اصلی و کدی خواهد بود که از طریق اس ام اس به تلفن شما ارسال می شود.



فیشینگ


www.dish2011.com/pgw.bpm.bankmellat.ir.pgwchannel.payment.mellat.RefId=
بانک ملت
bank mellat
دروازه پرداخت اینترنتی بانک ملت
نام پذیرنده
شرکت رایانمهر
مبلغ قابل پرداخت
960000 ریال
زمان باقیمانده 9:58
اطلاعات کارت
شماره کارت *
رمز اینترنتی کارت *
رمز دوم کارت (CVV2) *
تاریخ انقضای کارت
(ماه / سال)
حروف تصویر *
T6K27
0 9 3
5 7 6
2 8 4
Tab Back 1
صفحه کلید ابجدی
انصراف
پرداخت

برای درک مفهوم فیشینگ روند یک خرید سالم و طبیعی در اینترنت را مرور می کنیم:

روند طبیعی خرید های اینترنتی

برای پرداخت هزینه خرید به سایت بانک مراجعه می کند

خرید کالا انجام می گیرد

کاربر اطلاعات حساب خود را در سایت وارد می کند

کاربر قصد خرید اینترنتی دارد

حال نقش فیشینگ و نحوه کلا ... ایم:

روند فیشنگ در خرید های اینترنتی

کاربر قصد خرید اینترنتی دارد

کاربر برای پرداخت هزینه خرید خود به جای سایت بانک، به سایت جعلی مراجعه می کند

سارق اینترنتی صفحه جعلی خود را در دسترس دیگران قرار می دهد

خرید اینترنتی انجام نشده و اطلاعات حساب بانکی کاربر به دست فرد سارق اینترنتی می افتد

کاربر اطلاعات حساب خود را در سایت ...

سارق اینترنتی، سایت جعلی شبیه سایت بانک ایجاد می کند

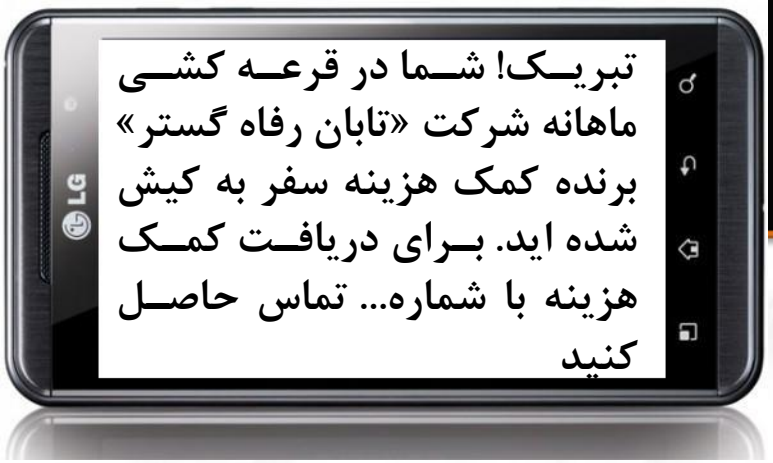
راههای پیشگیری از فیشینگ

سایت اصلی

سایت فیشینگ

۳) تصویر امنیتی در سایت فیشینگ ثابت و بدون تغییر باقی می ماند. اما در سایت اصلی بانک با هر بار کلیک بر روی فلش سبز رنگ، کد جدیدی تولید می شود.

پیامک برنده شدن



پیامک برنده شدن

فرد کلاهبردار پیامکی را با موضوع برنده شدن طراحی

قربانی در سودای برنده شدن جایزه با کلاهبردار تماس حاصل می کند

تبریک شما در قرعه کشی ماهانه شرکت «تابان رفاه گستر» برنده کمک هزینه سفر به کیش شده اید برای دریافت کمک هزینه با شماره... تماس حاصل کنید

فرد کلاهبردار قربانی را پای ه عابر کشانده و با ی های اشتباه کل دی حساب او را به ی برد

قربانی با ساده لوحی و اعتماد بی جا، زندگی خود را در چالشی بزرگ گرفتار می کند

رمز دوم


بانک ملت
bank mellat
6104 3370 7456 4585
محمدعلی خبوشان
CVV۲۶۳۵

رمز دوم

آنچه برای پرداخت هزینه ها از طریق اینترنت لازم دارید:

۱- شماره کارت

۲- کد CVV2

۳- تاریخ انقضاء

۴- رمز دوم

سارق برای سرقت اینترنتی تنها به رمز دوم شما نیاز دارد

رمز دوم

راههای بدست آوردن رمز دوم

ترفند اول) امانت گرفتن کارت و تعریف رمز دوم

ترفند دوم) فریب قربانی و پرسیدن رمز دوم از خود افراد

ترفند سوم) حدس زدن رمز دوم

در صورتی که سارق اینترنتی به هر نحوی رمز دوم کارت عابر بانک شمارا بدست آورد، براحتی خواهد توانست حساب بانکی شما را خالی کند.

خرید اینترنتی

خرید اینترنتی

مشکلات خرید اینترنتی

الف) تاخیر یا عدم تحویل کالا توسط فروشگاه های غیر مجاز

ب) تحویل کالا غیر مرغوب، تقلبی و دارای نقص

ج) مجرمانه بودن سایت و به سرقت بردن اطلاعات بانکی کاربر از طریق فیشینگ

د) ارائه کالا، مواد غذایی یا داروهای تاریخ گذشته و غیر بهداشتی و مضر

خرید اینترنتی

چگونه امنیت را در خرید اینترنتی تامین کنیم؟

نماد الکترونیکی نشان دهنده معتبر بودن فروشگاه های اینترنتیست که از سوی مرکز توسعه تجارت الکترونیکی صادر شده و با تعداد ستاره هایی که به فروشگاه تعلق می گیرد، میزان اعتبار و کیفیت خدمات و کالاهای ارائه شده توسط آن فروشگاه تایید می شود.

چگونه از واقعی بودن نماد الکترونیکی اطمینان حاصل کنیم؟

روی آیکن نماد کلیک کنید.

با این کار صفحه ویژه توضیحات مربوط به فروشگاه اینترنتی، در سایت enamad.ir باز شده و اطلاعات سایت به نمایش در می آید.

اسکیمر

اسکیمر

اسکیمر چیست؟

اسکیمر قطعه ای الکترونیکی است که مانند یک دستگاه کپی عمل کرده و از کارت عابر بانک شما کپی می گیرد.

این قطع
ورودی
و زمانی
خود را
اطلاعات
می کند.

اسکیمر

نحوه بدست آوردن رمز کارت

سارقین بعد از کپی کردن کارت شما به رمز آن هم نیاز دارند که آن را به یکی از روش های زیر بدست می آورند

۱) صفحه کلید مجازی

۲) تحت نظر قرار دادن شما

۳) نصب دوربین

اسکیمر

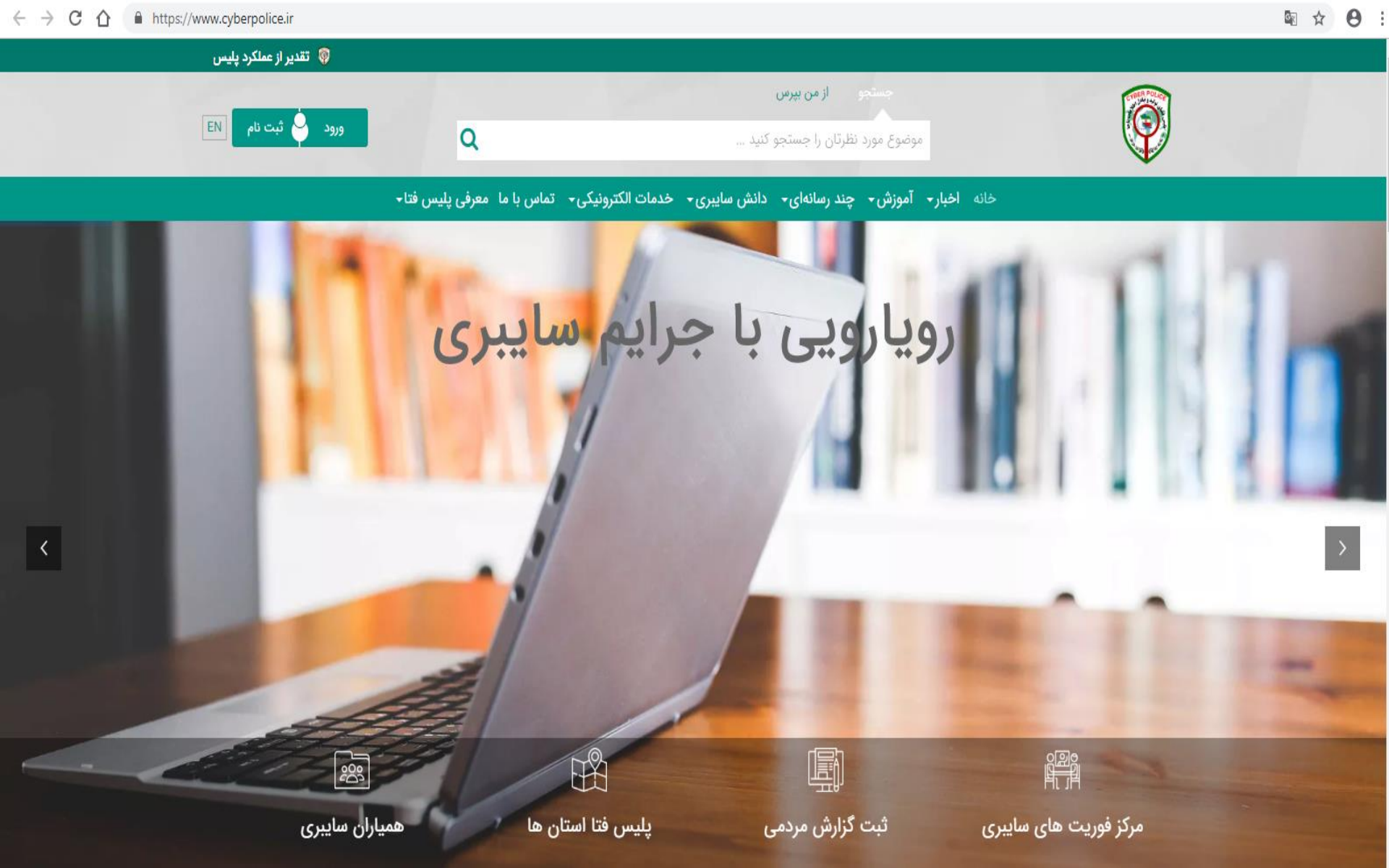
❖بنا بر این به خاطر داشته باشید...

۱- آنتی اسکیمر: قطعه ی پلاستیکی سبز رنگ که در درگاه ورودی دستگاه های خود پرداز نصب و باعث ایمن شدن دستگاه می شود.

۲- مراقب افراد مشکوک که اعمال شما را زیر نظر دارند باشید.

۳- مراقب تغییرات فیزیکی دستگاه باشید: در صورتی که کوچکترین تغییر غیر عادی در ظاهر (دوربین کوچک، صفحه کلید و...)و یا عملکرد دستگاه مشاهده کردید، به هیچ عنوان از دستگاه استفاده نکنید

سایت پلیس فتا



با تشکر از صبر و حوصله شما