امنیت در
فضای سایبری

امنیت

- امنیت مودم های وای فای
- امنیت رایانه های شخصی
- امنیت سیستم های مخابراتی
- امنیت شبکه های اجتماعی
- امنیت بانکداری الکترونیک
- امنیت خریدهای اینترنتی
- امنیت پیام رسانها






گام اول

امنیت اینترنت و مودم


WIRELESS
ROUTER

این روزها جلوگیری از هک وای فای با انتشار انواع ابزارهای هک وای فای بصورت کاملا جدی توصیه می شود.
جالب است بدانید هک وای فای به حدی سر زبان ها افتاده که بچه های کوچک نیز از این موضوع صحبت می کنند. توجه داشته باشید که مسئولیت اینترنت و آی پی مورد استفاده شما در لحظه هک شدن با شماست. یعنی اگر کسی وای فای مودم شما را هک و از آن استفاده غیر اصولی مانند فیشینگ و موارد مشابه کند در قبال این موضوع مسئول خواهید بود

لذا با رعایت نکات امنیتی زیر امنیت را برای بستر اینترنت ومودم خود فراهم نمائید

۱– برروی مودم خود پسورد ۸ کارکتری ویا بیشتر ترکیبی از اعداد وحرف وعلائم قرار دهید ضمن آنکه به صورت ماهانه نیز پسورد را تغییر دهید

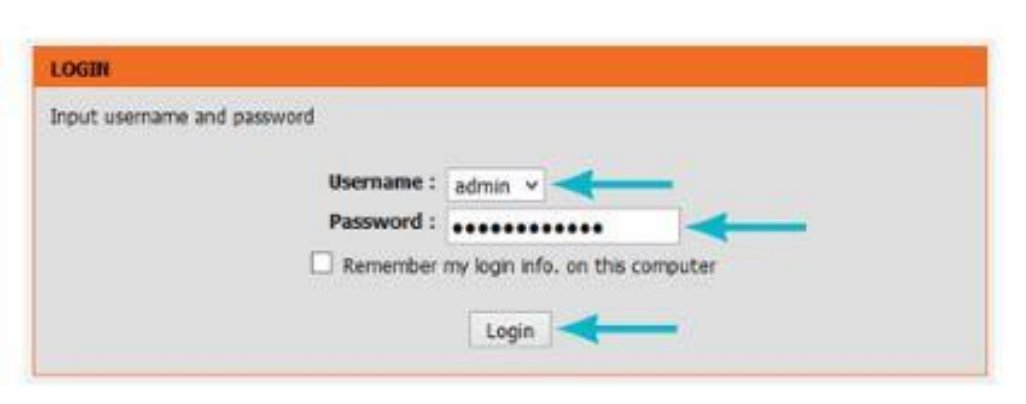
۲– مخفی کردن نام مودم خود از دید دیگر دستگاه‌ها با تغییر در تنظیمات SSID مودم

۳– تعداد دستگاههای استفاده کننده از مودم را محدود کنید

۴– کاربران برای تنظیم مودم خود با استفاده از دفترچه راهنمای مودم و یا سایت اپراتور اینترنتی یا شرکت سازنده مورد نظر می‌توانند تنظیمات مودم خود را انجام دهند ویا با مراجعه به سایت DLsoft.ir **فیلم تنظیمات مودم را مشاهده نمایید .**

۵– پسورد اینترنت وای‌فای خود را در اختیار میهمانان خود نگذارید و اگر پسورد اینترنت خود را به میهمان اعلام کردید سریعا بعد از پایان میهمانی پسورد اینترنت وای‌فای خود را تغییر دهید

۶– رمز عبور کنسول مدیریت مودم را در قسمت تنظیمات مودم تغییر دهید.



۷– درصورتی که از مودم استفاده نمی کنید آن ر ا خاموش کنید.

۸– برای انجام تنظیمات وای فای خود نیاز به آدرس صفحه تنظیمات مودم وای یا همان IP مودم خود داریم که این IP 192.168.1.1 می باشد

۹– برنامه هایی برای scan مودم وای فای آمده است که از طریق آن می توانید مشاهده کنید که چه کسانی به مودم شما وصل شده اند و دسترسی آنها را قطع کنید. یکی از بهترین برنامه های تجزیه و تحیل وای فای شبکه، در مارکت اندروید، Home alert proمی باشد.

۱۰– اتصال به اینترنت باز و رایگان بدون رمز عبور در امکان عمومی، به راحتی اطلاعات شما را در معرض رویت کسانی قرار می‌دهد که به همان منبع اینترنت متصل هستند

گام دوم

امنیت رایانه های شخصی

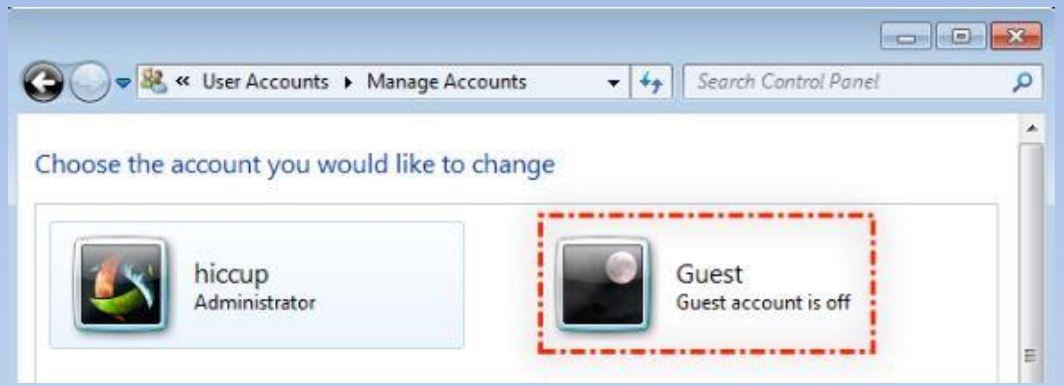

1 2 3
4 5 6
7 8 9
* 0 #

امنیت کامپیوترهای شخصی معمولا به دو جنبه کلی امنیت فیزیکی و نرم افزاری تقسیم بندی می گردند.
امنیت فیزیکی شامل مواردی از قبیل سرقت، شرایط نامساعد جوی، حوادث غیرمترقبه و سایر خطرات فیزیکی می گردد. در حالی که امنیت نرم افزاری می تواند جنبه های گسترده تری را شامل گردد که از مهم ترین آنها می توان به حملات فیشینگ، نفوذ هکرها،نرم افزرهای تبهکارانه، و.... اشاره نمود.
لذا توصیه می گردد موارد ذیل را در تامین امنیت سیستم رایانه شخصی خود رعایت نمایید .

۱– دوربین روی لپ تاب و یا وب کم رایانه خود رادر هنگام اتصال به اینترنت با برچسب ویا هرچیز دیگر بپوشانید

۲– فعال سازی دیوار آتش (Firewall) ویندوز

۳– غیرفعال سازی Guest Accountدر ویندوز



۴– برروی ویندوز خود از یک آنتی ویروس قوی مانند (Total security)استفاده نمائید

۵– بروزرسانی مرتب آنتی ویروس و سیستم عامل سیستم

۶– از قراردادن هرگونه اطلاعات شخصی برروی رایانه شخصی خود خودداری کنید

۷– اطلاعات مهم درون رایانه شخصی خود را درون هارد اکسترنال ویا فلش مموری نگهداری وبرروی آنها رمز گذاشته و درجایی امن نگهداری کنید

۸– به روز نگه داشتن نرم افزارهای مورد استفاده در سیستم کامپیوتر

۹– تهیه نسخه پشتیبان از اطلاعات و فایل های ضروری

۱۰– قطع ارتباط با اینترنت زمانی که از آن استفاده نمی گردد

۱۱– استفاده از مروروگرهای امن و مناسب

۱۲– عدم مشاهده و ذخیره فایل های پیوست شده ناشناس در ایمیل ها

گام سوم

امنیت
تلفن همراه

تلفن‌های هوشمند امروزی، علاوه بر قابل‌حمل بودن، اطلاعات شخصی ما را هم با خود حمل می کنند! امروزه امنیت مسئله بزرگی است که شکسته‌شدن آن برای تلفن شما چیزی بیش ازدست دادن چند شماره تلفن خواهدبود.

ما درباره حساب‌های شبکه‌های اجتماعی، فایل‌های شخصی و محرمانه، اسناد مهم، ایمیل‌ها، تصاویر و پیام‌ها و چندین و چند مورد دیگر صحبت می‌کنیم.

در این بین اندروید سیستم‌عاملی فراگیر و رایج است که کاربران بسیاری از آن استفاده می‌کنند، اساس اندروید هم منبع کاملاً باز یا به اصطلاح Open Source**بودن است که به خودی خود می‌تواند امنیت گوشی شما را پایین بیاورد.**

لذا با رعایت نکات زیر امنیت تلفن همراه خود را فراهم نمایید .

۱– بروی گوشی های دارای سیستم عامل اندروید خود از یک آنتی ویروس قوی مانند (Security Mobile)استفاده نمائید

۲– برروی گوشی و تبلت خود رمزهای پیچیده وغیر قابل حدس بگذارید و با انتخاب یکی از روش های Pattern, PIN, ، Password امنیت آن را بالا ببرید

۳– با تبلت و گوشی به هیچ عنوان اطلاعات محرمانه خود را رد و بدل نکنید و سعی کنید برای این کار از یک کامپیوتر مطمئن استفاده کنید

۴– به هیچ عنوان با تبلت ویا گوشی خود که دارای اطلاعات محرمانه است از اینترنتهای وای فای رایگان در اماکن عمومی استفاده نکنید ویا امورات مهم ومحرمانه خود را با استفاده از این اینترنتهای وای فای رایگان انجام ندهید

۵– از قرار دادن هرگونه اطلاعات شخصی برروی تبلت و گوشی خودداری نمائید وتاقبل ازاینکه گوشی ویا تبلت شما مفقود ، سرقت یا هک ویا خراب شود اطلاعات مهم درون آن را خارج نمائید .

۶– اطلاعات مهم درون گوشی ، تبلت ولپ تاب خود را درون هارد اکسترنال ویا فلش مموری نگهداری وبرروی آنها رمز گذاشته و درجایی امن نگهداری کنید

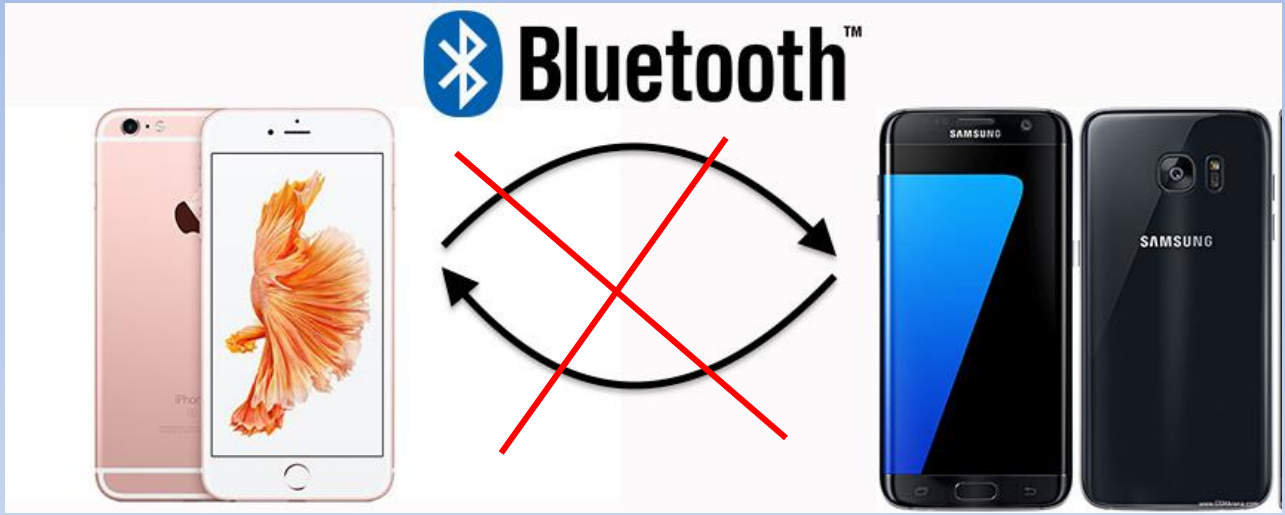
۷– برای تمام برنامه های خود passwordبگذارید نرم افزارهایی چون applockاین کار را به راحتی برای شما، انجام خواهندداد

۸– برروی گوشی خود نرم افزارهای مکان یاب مانند (Find My Phon) نصب نمائید تا در زمان سرقت و یا مفقودی گوشی خود را در اسرع وقت پیدا نمایید

۹– هنگامی که گوشی را برای تعمیر می برید حتماً تمامی اطلاعات آن را به طور کامل تخلیه نمایید و آن را به تعمیرکاران باتجربه و قابل اعتماد بدهید .

۱۰– استفاده از Wi-Fi و Blue tooth را محدود کنیدو زمانی که نیازی نیست آن را خاموش نمایید

۱۱– بلوتوث گوشی خودرا همیشه خاموش نگه دارید و از دریافت بلوتوثهای ناشناس خودداری کنید



۱۲– از اطالعات گوشی ویا تبلتتان ، یک نسخه پشتیبان بگیرید

۱۳– به هیچ عنوان اجازه ندهید افراد غریبه ویا کسانی که نمی شناسید از اینترنت شخصی شما چه برروی سیستم وچه برروی موبایل استفاده نمایند

۱۴– هیچگاه با گوشی ویا تبلت دیگران امورات مهم وشخصی خود ازقبیل تراکنشهای بانکی ، وارد شدن به ایمیل وصفحات شخصی خودرا انجام ندهید

۱۵– درصورتی که گوشی شما سرقت شد بعد از انجام شکایت در مراجع قانونی می توانید با شماره گیری #۶۱۰۱* از سیستم ردیابی ایرانسل و باشماره گیری #۲۱۴۳*۱۰* با ارسال سریال گوشی مندرج برروی جعبه گوشی از سیستم ردیابی سیم کارتهای دائمی همراه اول استفاده نمائید

۱۶– درصورتی که جعبه گوشی خودرا گم کرده اید ونیاز به سریال گوشی خود دارید می توانید بازدن کد #۰۶#* سریال گوشی (IMEI) را مشاهده نمائید

گام چهارم

امنیت
شبکه های
اجتماعی


twitter
Google Buzz
MySpace
tumblr
reddit
Blogger

یکی از تاثیر گذارترین سرویس‌های ارائه در اینترنت، شبکه‌های اجتماعی هستند که به نوبه خود تحول شگرفی را در نظام اجتماعی دنیا ایجاد کرده است .

این شبکه ها علاوه بر ویژگی هایی که دارند دارای معایبی هم می باشند از قبیل جاسوسی ، اعتیادبه این شبکه ها ، افت تحصیلی دانش آموزان ، کم رنگ شدن روابط عاطفی در خانواده ها و غیره .

علاوه بر معایبی که مطرح شد عدم آگاهی از استفاده صحیح از این شبکه ها وعدم تامین امنیت این شبکه ها از سوی کاربران ممکن است خطرات ودردسرهایی برای آنها ایجاد نماید .

به علت پر طرفدار بودن شبکه اجتماعی تلگرام دربین مردم در ادامه جهت استفاده از شبکه های اجتماعی به ویژه تلگرام توصیه می شود نکات امنیتی زیر را رعایت نمائید :

۱– برروی شبکه اجتماعی تلگرام نصب شده رمز عبور بگذارید برای اینکار مراحل زیر را انجام دهید :

۱- وارد برنامه تلگرام شوید.
۲- به قسمت تنظیمات (settings) وارد شوید.
۳- گزینه privacy and security را انتخاب کنید.
۴- گزینه passcode lock را انتخاب کنید.
۵- در این مرحله رمز مورد نظر خود را وارد کنید.
۶- عملیات رمزگذاری در این مرحله به پایان رسیده است و در قسمت بالا آیکون قفل باز ظاهر شده است.

اما این امکان وجود دارد که هنگام خروج فراموش کنید روی قفل کلیک کنید که اگر بخواهید به صورت اتوماتیک این کار انجام شود در قسمت password lockگزینه Auto lockرا انتخاب و مقدار آن را به زمان دلخواه خود تغییر دهید تا در زمان تنظیم شده به طور اتوماتیک تلگرام قفل شود

۲– برروی شبکه اجتماعی تلگرام نصب شده رمز دومرحله ای (two–step verification) بگذارید برای اینکار مراحل زیر را انجام دهید :

۱– وارد برنامه تلگرام شوید.
۲– به قسمت تنظیمات (settings) وارد شوید.
۳– وارد قسمت privacy and security شوید.
۴– گزینه two–step verification را انتخاب نمایید.
۵– روی گزینه set additional password کلیک کنید.
۶– در این قسمت Email و Password را با دقت وارد کنید چرا که این پسورد در آینده برای شما نیاز خواهد بود.
پس از وارد کردن پسورد و ایمیل با پیغام زیر روبه رو می شوید که می بایست ایمیل خودتان را چک کنید

Please check your email to compelete two–step verification

۷– ایمیل ارسالی دارای یک لینک می باشد که کلیک بر روی آن به منزله تایید است و شما باید این کار را انجام دهید تا عملیات انجام شده با موفقیت ثبت شود. پس از کلیک روی لینک تصویر زیر را مشاهده خواهید کرد.

حال اگر کسی قصد ورود به تلگرام با شماره شما را داشته باشد اگر کد ارسال شده توسط تلگرام را داشته باشد نیاز به پسوردی که در این مرحله تعین کرده اید دارد تا بتواند وارد اکانت شما شود

۳– محیط شخصی تلگرام خود را از حضور افراد غریبه پاکسازی نمایید برای انجام این کار مراحل زی را انجام دهید :

۱– وارد برنامه تلگرام شوید
۲– به قسمت تنظیمات (settings) وارد شوید.
۳– وارد قسمت privacy and security شوید.
۴– به قسمت active sessions وارد شوید.
۵– در این قسمت مشاهده می کنید که دستگاه دیگری نیز از این اکانت استفاده می کند که این موضوع در صورتی که توسط شما انجام نشده باشد امنیت تلگرام شما را به خطر می اندازد چون تمام اطلاعات ارسالی و دریافتی دیگر ما از طریق شخص دیگری در حال رصد شدن می باشد که امکان سواستفاده از آن میسر می شود.
۶– اگر بخواهید کاربری که از اکانت شما استفاده می کند را از اکانت خارج کنید دستگاه مورد نظر را انتخاب و گزینه ok را بزنید.
۷– اگر بخواهید همه کاربران اضافی را از اکانت خارج کنید گزینه Terminate All Other Sessionsرا انتخاب و ok کنید.

۴– عدم نمایش آنلاین بودن شما در تلگرام از دید دیگران جهت انجام این کار مراحل زیر را انجام دهید :

۱– وارد برنامه تلگرام شوید.
۲– به قسمت تنظیمات (settings) وارد شوید.
۳– وارد قسمت privacy and security شوید.
۴– گزینه Last Seen را انتخاب کنید.
۵– در قسمت اول ۳ گزینه وجود دارد که Everybody اشتراک عمومی بوده و همه می توانند آنلاین بودن شما را رویت کنند.
۶– گزینه دوم My Contacts نفراتی که شماره آنها در دفترچه تلفن شما ذخیره شده است می توانند مشاهده کنند.
۷– گزینه سوم Nobody بوده و هیچ کس نمی تواند زمان آنلاین بودن شما را مشاهده کند.

۵– مسدود کردن کاربران مزاحم در تلگرام (Block Users)

با استفاده از این امکان می‌توان افرادی را که برای کاربر ایجاد مزاحمت می‌کنند و یا شماره تماس‌های ناشناسی که با ارسال تبلیغات ناخواسته و هرزنامه‌ها موجب اتلاف زمان و انرژی کاربر می‌شوند را انتخاب و مانع مشاهده‌شدن توسط آنان شد.

با وارد شدن به بخش Block Users که در آن تمامی کسانی که شماره کاربری آنها توسط کاربر فیلتر شده اند قابل مشاهده خواهد بود.

با انتخاب علامت + در بالای صفحه کاربر وارد دفترچه تلفن خود به شکل زیر می شود که می تواند از آن لیست، افرادی را که می خواهد مانع ارتباط آنان در تلگرام شود انتخاب کند.

در صورت تمایل به خارج کردن افراد از لیست فیلترشده کاربر می‌تواند با انتخاب فرد و و استفاده از گزینه Unblock وضعیت ارتباطی با فرد را به حالت طبیعی باز گرداند.

۶– از بین رفتن حساب کاربری تلگرام (Account self-destructs)

یکی از ویژگی‌های منحصربه‌فرد تلگرام امکان از بین بردن حساب کاربری و اطلاعات و محتوای آن به‌صورت خودکار است که این امکان را به کاربر می‌دهد در صورت عدم فعال‌بودن در مدت‌زمان تعریف‌شده توسط او حساب کاربری به شکل خودکار از بین رفته و امکان دسترسی و سو استفاده دیگران موجود نباشد.

برای اینکار می توانید با وارد شدن به قسمت settings سپس قسمت privacy and security و سپس در قسمت Account self-destructs مدت زمان پیش‌فرض برای از بین رفتن حساب کاربری را کاهش و یا افزایش دهید .

۷- گفتگوی محرمانه در تلگرام

گفتگوی محرمانه در تلگرام یکی از ویژگی‌های بسیار خوب این نرم‌افزار برای محافظت از حریم خصوصی و امنیت کاربران است

ویژگی‌های اصلی این نوع گفتگو در تلگرام به شرح زیر است:

❋پیامها به صورت سرتاسری رمزنگاری می‌شود. یعنی پیغام‌های ارسالی از ابتدای مسیر تا رسیدن به مقصد رمزشده هستند

❋در دستگاه‌های دیگر که در آن‌ها از تلگرام استفاده می‌کنید دیده نمی‌شوند

❋

گفتگوهای انجام‌شده دارای یک زمان‌بندی برای تخریب هستند و بعد از گذشت زمان معینی از بین می‌روند

برای انجام گفتگوی محرمانه با یکی از افراد موجود در لیست مخاطبان، ابتدا وی را در لیست مخاطبان انتخاب کنید. با انجام این انتخاب آخرین صفحه مکالمات اخیری که با هم داشته‌اید نمایش داده می‌شود. سپس قسمت بالای صفحه که نام مخاطب یا شماره وی همراه با تصویر نمایه وی قرار دارد را انتخاب کنید.

پس از انتخاب، مشخصات مخاطب مورد نظر نمایش داده می‌شود. در این صفحه با انتخاب گزینه Start Secret Chatیک گفتگوی محرمانه میان شما و مخاطب مورد نظر ایجاد می‌شود.

۸- ازبین بردن حساب کاربری تلگرام درصورت مفقود شدن یا سرقت گوشی

گاهی اوقات برای کاربران تلگرام اتفاق افتاده است که گوشی ویا تبلتی که بروی آن حساب کاربری تلگرام دارند به سرقت رفته یا آن را گم کرده اند برخی از کاربران در این شرایط نمیدانند برای حف حساب کاربری خود برروی گوشی مفقود شده چه باید بکنند با انجام مراحل زیر حساب کاربری خودرا از روی گوشی ؛ تبلت ویا لپ تاب مفقودی حذف نمائید :

۱- ابتدا سیم کارت گوشی مفقودی را بسوزانید.

۲- سیم کارت جدیدی با همان شماره قبلی را برروی گوشی جدید نصب نمائید

۳- مجددا تلگرام را با همان شماره قبلی روی گوشی جدید نصب نمائید

۴- اکنون شما ۲ حساب کاربری با یک شماره موبایل دارید یکی روی گوشی جدید ویکی برروی گوشی مفقودی .

۵- در تلگرام جدید که نصب نمودید وارد قسمت تنظیمات (settings) وارد شوید.

۶- گزینه privacy and security را انتخاب کنید.

۷- به قسمت active sessions وارد شوید.

۸- در این قسمت مدل گوشی ؛ تبلت یا لپ تاب مفقودی که حساب کاربری شما برروی آن نصب شده را مشاهده می کنید دستگاه مورد نظر را انتخاب وOK را بزنید حساب کاربری تلگرام شما از روی آن حذف می شود

۹– پاک کردن حساب کاربری تلگرام از روی گوشی

بعضی از کاربران شبکه اجتماعی تلگرام جهت پاک کردن تلگرام نصب شده روی گوشی ؛ تبلت ویا لپ تاب خود به اشتباه وارد قسمت تنظیمات گوشی خود شده وگزینه لغو نصب را زده و به خیال خود حساب کاربری تلگرام خود را پاک می نمایند که این را کاملا اشتباه می باشد برای اینکار می بایست مراحل زیر را انجام دهید :

۱– وارد سایت تلگرام به این آدرس شوید :

https://my.telegram.org/auth?to=deactivate

۲– شماره موبایلی که با آن تلگرام را نصب نمودید در این قسمت وارد نمائید

۳– شرکت تلگرام همان لحظه کد ۱۱ رقمی در تلگرام شما ارسال می نماید

۴–این کد را در این سایت وارد نمائید از شما سوال پرسیده می شود که چرا می خواهید حساب کاربری را پاک نمائید که شما هر جوابی بخواهید می توانید بدهید .

۵– درپایان ۲ گزینه درمقابل شما قرار می گیرد (Yes Delet account) به رنگ قرمز و (No Delet account) به رنگ سبز که بازدن گزینه Yes حساب کاربری شما بطور کامل از شرکت تلگرام وگوشی شما پاک می گردد .

۱۰– ایجاد نکردن حساب کاربری تلگرام با سیم کارتی که سند آن بنام شما نیست

بعضی از کاربران شبکه اجتماعی تلگرام گاهی اوقات با سیمکارتی شبکه اجتماعی تلگرام را نصب می نمایند که سند سیم کارت بنام آنها نیست که این امر بعدها ممکن است برای صاحب آن حساب کاربری مشکلاتی را ایجاد نماید . بعنوان مثال اگر صاحب سیمکارت بدون هماهنگی شما سیمکارت را بسوزاند وبا آن سیمکارت برروی گوشی خود تلگرام نصب نماید تلگرام شما دراختیار او قرار می گیرد ومی تواند به همه چتهای شما واعضای تلگرام شما دسترسی پیدا نماید . برای جلوگیری از بوجود آمدن چنین خطراتی به کاربرانی که با سیمکارتی که سند آن بنام آنها نیست توصیه می شود به مراحل زیر عمل نمایند :

۱– تاریخچه تمامی چتهای اعضای گروه را پاک نموده در قسمت (Clear History) تلگرام

۲– تمامی عکسهای شخصی پروفایلتان را پاک نموده

۳– تلگرامی که با این سیمکارت نصب نموده اید را از طریق سایت تلگرام Delet account نمائید

۴– سیمکارت جدیدی تهیه نمائید که سند آن بنام شما باشد و حساب کاربری جدیدی در تلگرام با آن ایجاد نمایید

۱۱– برروی گوشیی شبکه های اجتماعی را نصب نمائید که درون آن هیچگونه اطلاعات مهم وشخصی وجود نداشته باشد

۱۲– برروی گوشیی که شبکه اجتماعی نصب می کنید رمز عبور پیچیده بگذارید

۱۳– برروی گوشی که قصد دارید شبکه اجتماعی نصب نمائید یک آنتی ویروس قوی (security mobile **) نصب نمائید**

۱۴– از ارسال شماره کارت ورمزهای آن در شبکه های اجتماعی برای دیگران بپرهیزید

۲۰– از باز نمودن لینکهای مشکوک در شبکه های اجتماعی خودداری کنید

۲۲– لینک هایی که با پسوند (bot.) **می باشد اعتماد و لمس نکنید زیرا این لینک ها ربات بوده و احتمال بدافزار بودن آنها وجود دارد**

۲۲– از هرگونه خرید از افراد ناشناس درشبکه های اجتماعی خودداری کنید و درصورت خرید یک کالا ابتدا جنس را تحویل گرفته وپس از اطمینان از صحت کالا وجه آن راپرداخت نمائید

۲۳ – از قرار دادن تلفن همراه ، تبلت یا رایانه شخصی خود به دیگران خوداری کنید

گام پنجم

امنیت
در بانکداری
الکترونیک


Credit Card
0000 0000 0000 0000
07/20
NAME SURNAME
1234
NAME SURNAME
NAME SURNAME

۱– رمز کارت خود را در مدت زمانها معین تغییر دهید

۲– کارت خود و رمز آن را در اختیار دیگران قرار ندهید

۳– به هیچ عنوان از دیگران جهت پرداخت قبوض یا برداشت پول از کارت خود استفاده نکنید

۴– پس از دریافت کارت از شعب بانک بلافاصله رمز عبور آن را از طریق دستگاه های خودپرداز آن بانک تغییر دهید

۵– ازنوشتن رمز عبور بر رو یا پشت کارت یا نگهداری آن در مجاورت کارت جداً خودداری شود

۶– از پذیرش هرگونه درخواست افراد ناشناس به منظور استفاده از خدمات بانکی به واسطه کارت شما اکیداً خودداری شود

۷– تماس‌های تلفنی، پیامکی و همچنین از طریق شبکه های اجتماعی از بازگو کردن مشخصات محرمانه خصوصی کارت بانکی (رمزها، کد اعتبارسنجی و تاریخ انقضاء) برای دیگران خودداری کنید

۸– درصورت گم شدن کارت بانکی فورا آن رامسدود نمائید

۹– درصورتی که کارت شما درزمانی مفقود شد که دسترسی به بانک عامل راندارید به دوروش آن رامسدود نمائید
الف: ازطریق تلفن بانک

ب: به دستگاه ATMبانک عامل کارت خود مراجعه نموده دکمه ثبت برروی صفحه کلید را یکبار فشار دهید خدمات بدون کارت فعال می گردد سپس در قسمت مسدود کردن کارت شماره کارت ورمز کارت مفقود شده را وارد وکارت خود را مسدود نمائید

۱۰– شماره ۱۶ رقمی کارت خود را برروی گوشی خود ذخیره نمائید

۱۱– برای جلوگیری از کپی برداری افراد سودجو از کارت شما هنگام خرید با دستگاه پوز کارت راخودتان بکشید ورمز کارتتان راخودتان بزنید

۱۲– در هنگام استفاده از ATMدر هنگام وارد کردن رمز کارت دست خود را برروی صفحه کلید نگهدارید تا رمز وارد شده دیده نشود

۱۳– هنگامی که وارد یک درگاه بانک در اینترنت می شوید از درست بودن آدرس بانک و داشتن https در آدرس سایت وجود تصویر امنیتی وجود صفحه کلید مجازی وفعال بودن آن اطمینان حاصل نمائید

۱۴– درصورتی که به شما پیامک داده شد ویا تماس گرفته شد که شما برنده شده اید وجهت دریافت جایزه به کنار دستگاه خودپرداز مراجعه کنید اینکار رانکنید چون این افراد کلاهبردار هستند

گام ششم

امنیت
در خریدهای
اینترنتی

۱– از سایت هایی خرید نمایید که حتماً نماد اعتماد الکترونیکی را داشته باشند. در حال حاضر نزدیک به3000 کسب و کار اینترنتی دارای نماد هستند که در سایت Enamad.ir قابل مشاهده است

۲– نماد اعتماد الکترونیکی با یک آرم مشخص در صفحه‌ی نخست سایت مورد نظر قابل مشاهده است که جهت بررسی اصالت آن نماد می توان روی آن کلیک کرده و اطلاعات فروشگاه را در آنجا مطالعه نمایند

نماد اعتماد الکترونیکی
www.eNAMAD.ir

۳– وقتی خرید اینترنتی انجام می دهید استفاده از پرداخت نقدی بعداز تحویل کالامی تواند به افزایش سطح امنیت کمک کند

۴– درصورت خرید یک کالا در اینترنت ابتدا جنس را تحویل گرفته وپس از اطمینان از صحت کالا وجه آن راپرداخت نمائید

گام هفتم

هکرها و راهکار های مقابله

گاهی هکرها از طریق ایمیل‌های اسپم و .....کاربران برای کلیک کردن بر روی لینک‌های مخرب فریب داده می‌شوند، سپس باج افزار، سیستم‌های رایانه‌ای و دستگاه‌های یا فایل‌های آن‌ها را غیر قابل دسترس می‌سازد و در واقع آن‌هاراگروگان می‌گیرد تا قربانی باج مربوطه را پرداخت نماید.

برای اینکه باجی به هکرها ندهیم چه باید بکنیم؟

۱– تهیه فایل پشتیبان از اطلاعات مهم خود

۲– تنظیم یک برنامه برای بک‌آپ گیری مناسب

۳– نسبت به ایمیل‌های جعلی (فیشینگ) آگاهی داشته باشید

۴– به روز رسانی نرم افزارها کاربردی رایانه خود

۵– اطلاعات شخصی و اطلاعات کاری خود را از هم جدا سازید

گام هشتم

نظارت والدین برفرزندان

اینترنت می‌تواند مکانی گسترده برای کودکان باشد تا بیاموزند، سرگرم شوند، با دوستان مدرسه‌ای گپ بزنند، و با آسودگی خیال به مکاشفه بپردازند. اما درست همانند دنیای واقعی، وب هم می‌تواند برای کودکان خطرناک باشد. قبل از اینکه به کودکانتان اجازه دهید که بدون نظارت شما به اینترنت متصل شوند، موارد زیر را رعایت نمائید :

۱– رایانه را در جایی از خانه قرار دهید که امکان نظارت وکنترل والدین بر فرزندان وجود داشته باشد

۲– به فرزندان خود بیاموزید افرادی که در فضای مجازی با آنها آشنا می شوند ممکن است آن شخصی که معرفی می کنند نباشند

۳– به فرزندان خود بیاموزید که در فضای مجازی از باز نمودن ایمیل های مشکوک خودداری کنند

۴– به فرزندان خود بیاموزید : به دوستان خود محبت کنند ولی به آنها اعتماد نکنند

۵– به فرزندان خود بیاموزید به درخواست کاربرانی که نمی شناسندپاسخ ندهند و به هیچ عنوان اطلاعات شخصی خود را برای آنها ارسال نکنند

۶– هرگز با کسی که در اینترنت آشنا شده‌اید قرار حضوری نگذارید، مگر اینکه هویت واقعی وی برای شما احراز شود و والدین شما در جریان این قضیه باشند.

۷ – از موتور جستجوی ایمن برای کودکان استفاده نمائید
وب سایت www.KidRex.orgدر واقع موتور جستجوی سفارشی گوگل برای بچه ها است.
محیط صفحه اصلی درست مثل نقاشی مداد رنگی یا مداد شمعی کودکانه است (با یک دایناسور محافظ!).

۸– به فرزندانتان تأکید کنید که هرگز آدرستان، شماره تلفن یا سایر اطلاعات شخصی شامل جایی که به مدرسه می‌روند یا جایی که دوست دارند بازی کنند را ارسال نکنند.

در پایان به این نکات توجه داشته باشید :

۱– انگیزه سایتهای شرط بندی ، کلاهبرداری بوده و تنها با هدف دریافت پول از کاربران خود طراحی شده اند

۲– در صورت مواجه با موارد مشکوک می‌توانید آن را از طریق سایت پلیس فتا به آدرس Cyberpolice.irبخش مرکز فوریت‌های سایبری، لینک ثبت گزارشات مردمی به پلیس فتا اعلام نمایید.

۳– برای ارتباط گرفتن با کارشناسان پلیس فتا می توانید با گرفتن شماره تلفن ۱۱۰ به کارشناسان پلیس فتا متصل شوید

۴– درصورتی که اتفاقی برای شما در فضای مجازی افتاد سریعا به دادسرای جرایم رایانه ای محل سکونت خود مراجعه نمایید .