www.cyberpolice.ir

هر آنچه برای امنیت مجازی لازم است

بیاموزیم

امنیت اشتراک گذاری

امروزه شاید یک از جذاب ترین فعالیت هـای روزانـه افـراد اشتراک گذاری مطالب گاها حساس خود می باشد که بی مهابا و بدون رعایت نکات امنیتی آنها را نشر مـی دهنـد .پـیش از انتشار مطالب نکات زیر را رعایت نمایید

۱– پیش از تصویر برداری، GPS تلفن همراه خود را غیر فعال نمایید تا در هنگـام اشتراک گذاری تصاویر موقعیت مکانی شما نامعلوم بماند.

۲– تصاویر و ویدیو های خود را به هیچ عنوان برای افراد ناشناس ارسال ننمایید.

۳– در صورت لزوم به ارسال تصـاویر و ویـدیو پـیش از بارگـذاری تنظیمـات محرمانگی (privacy) حریم خصوصی خود را کنترل نمایید.

۴–هرگز اطلاعات مهم شخصی (شماره کارت های بانکی،کد ملی ،رمز عبـور و...) را در هیچ محیطی بارگذاری ننمایید.

امنیت
مرور گر های وب

کار بران در سنین مختلف دارای نیازمندی هایی خاص در بستر اینترنت می باشند که مجاب به استفاده از مرورگر میباشند که بدون رعایت نکات امنیتی زیر ممکن است خطراتی را پیش رو داشته باشند:

۱- همواره مرورگر خود را به روز نگاه دارید.

۲- از مرورگرهای شناخته شده استفاده نمایید.

۳- تا حد ممکن کلمه‌های عبور را ذخیره ننمایید مخصوصاً در اماکن عمومی که میتواند در اختیار دیگران قرار گیرد.

۴- هرگز نرم افزارهای تبلیغاتی را بر روی سیستم خود نصب ننمایید.

۵- از تائید نمودن درخواست های ناشناس در مرورگرهای وب خودداری نمایید.

امنیت پست الکترو نیک

اطلاعاتی را که در یک پست الکترونیکی ارسال می شود ممکن است دارای ارزش زیادی باشد که شاید آن را به یک هدف برای هکر ها تبدیل نماید. در زمانی که از پست الکترونیک استفاده می نمایید از توصیه های زیر استفاده نمایید

۱- در ارسال پیام به صورت گروهی مراقب باشید اطلاعات را به چه افرادی ارسال می نمایید. (لیست گروه خود را چک نمایید)

۲- جهت امنیت بهتر ایمیل ، از یک آنتی ویروس بروز و معتبر استفاده نمایید.

۳- به هیچ وجه ایمیل های حساس و حاوی اطلاعات مهم خود را از طریق اینترنت های رایگان و یا عمومی بررسی ننمایید.

۴- هرگز ایمیل های هرزه (اسپم) که منبع معتبری ندارد را باز ننمایید زیرا می تواند حاوی بد افزار باشد.

امنیت پیام رسان ها

در دنیای امروز بسیاری از فعالیت های روزانه ما از طریق پیام رسان های اینترنتی صورت می پذیرد و گاها شاهد می باشیم که بسیاری از کاربران بدون رعایت نکات امنیتی زیراقدام به ارسال مطالب محرمانه می نمایند

۱- همواره از بروز ترین نرم افزارهای پیام رسان استفاده نمایید.

۲- تصاویر پروفایل خود را به گونه ای انتخاب نمایید که دیگران فرصت سوء استفاده از آن را پیدا ننمایند.

۳- به هیچ وجه در پیام رسان ها رمز عبور و شماره کارت های بانکی را به شماره های ناشناس ارسال ننمایید.

۴-مطالب منتشر شده در شبکه های اجتماعی به هیچ نحوی قابل بازگشت نمی باشند پس مراقب باشید که چه مطالبی را بارگذاری می نمایید.

امنیت تلفن همراه

تلفن های همراه بدون شک به عضو لاینفک و جـدایی ناپـذیر زندگی ما تبدیل گردیده است که مزایای فراوانی برای انسـان دارد اما در کنار این فواید معایبی هم دارد که بدون رعایـت نکات امنیتی زیر نمی توان به راحتی از کنار آن گذشت:

۱- برای در امان ماندن از بدافزارهای تلفن همراه همواره از آنتی ویروس هـای مخصوص تلفن همراه استفاده نمایید.

۲- در زمان هایی که ابزار های مربوط به تلفـن همـراه (بلوتـوث،وای فـای و...)استفاده نمی نمایید آنها را غیر فعال نمایید.

۳- به پیامک هایی که از شما به هر طریقی شماره کارت هـای بـانکی را طلـب می نماید پاسخ ندهید.

۴-جهت جلوگیری از ورود بدافزار به تلفن همراه، نرم افزار های مورد نیاز خـود را از سایت های معتبر دانلود نمایید.

حفاظت از اطلاعات

هر فردی در زندگی شخصی خود دارای اسرار محرمانه و منحصر به فرد میباشد .کاربران باید بدانند که اطلاعات در صورت ورود به اینترنت از دسترس آنها خارج گردیده است از این رو هر کاربر برای حفظ اطلاعات شخصی خود باید نکات زیر را رعایت نمایند

۱- همانطور که برای امحاء کاغذ های حاوی اطلاعات محرمانه ، آن ها را به دستگاه های خرد کن می ریزیم اطلاعات رایانه ای حساس را با نرم افزار های امحاء از بین ببریم.

۲- در خریدهای اینترنتی از فروشگاه های دارای نماد الکترونیک خرید نمایید.

۳- از انتشار اطلاعات محرمانه و مهم در شبکه های اجتماعی حتی برای افراد با درجه اعتبار بالا خودداری نمایید.

۴- جاسوس‌افزارها، در رایانه‌ها به دنبال اطّلاعات حسّاس می‌گردند؛ نرم‌افزارهای امنیتی را برای کاهش آسیب به کار گیرید.

امنیت
خرید های آنلاین

زندگی امروزبا وجود اینترنت و شبکه های اجتماعی رنگ و بوی متفاوتی نسبت به گذشته گرفته و زمان هزینه و..حرف اول را میزنند . مردم بسیاری از امورخود را ازطریق اینترنت انجام می دهند که عدم توجه به نکات امنیتی زیر خطرات غیر جبرانی را در پیش دارد:

۱–فروشگاههای معتبر مشخصات واقعی را به طور دقیق در وب سایت خود درج می‌کنند.

۲– در هنگام خرید نسبت به پیشنهادهای وسوسه انگیز هوشیار باشید.

۳– به فروشگاه هایی که قیمت اجناس آنها زیر قیمت اصلی بازار می باشد مشکوک باشید.

۴– از سایت هایی خرید نمایید که از نماد اعتماد الکترونیکی استفاده نمایند.

۵– علاوه بر خرید از وب سایت‌های قابل اعتماد، از امنیت سیستم یا رایانه‌ای که از آن خرید آنلاین خود را انجام می‌دهید مطمئن باشید.

امنیت
در طول سفر

با ورود بستراینترنت به زندگی روزمره ما امنیت دیگر معطوف به دنیای واقعی نمیشود. در گذشته امنیت سفر معطوف به نگهداری منزل در سفر بود اما امروزه در صورت عدم رعایت نکات امنیتی زیر ممکن است خطرات جبران ناپذیری برجای بگذارد:

۱– در صورت عدم استفاده ازاینترنت تلفن همراه در سفر گزینه وای فای را غیر فعال نمایید.

۲– پیش از انجام سفر و قبل از خرید بلیط از جعلی نبودن درگاه پرداخت اینترنتی اطمینان حاصل نمایید.

۳–مراقب باشید در دام تورهای مسافرتی جعلی با پیشنهاد های اغوا کننده گرفتار نشوید.

۴– در طول سفر دستگاه بلوتوث و GPS تلفن همراه را خاموش نمایید.

امنیت فروشگاه های اینترنتی

در دنیای مدرن با توجه به اهمیت زمان بسیاری از مردم ترجیح می دهند خرید های خود را از فروشگاه های اینترنتی انجام دهند اما باید بدانیم فروشگاه های اینترنتی در صورت عدم رعایت نکات امنیتی زیر خطرات جبران ناپذیری بر جای می گذارد:

۱- پیش انجام خرید از فروشگاه های اینترنتی حتما صحت اطلاعات موجود در تماس با ما را بررسی نمایید.

۲- اطمینان حاصل نمایید که در صورت عدم دریافت بسته سفارشی امکان مراجعه حضوری وجود داشته باشد.

۳- پیش از خرید حتما بررسی نمایید فروشگاه مورد نظر دارای نماد اعتماد الکترونیکی(enamad) **باشد.**

۴- حتما بررسی گردد که فروشگاه مورد نظر، از پروتکل https **استفاده نمایند.**

۵- بررسی نمایید تا فروشگاه مورد نظر تصاویر واقعی از کالای مورد نظر را در سایت قرار داده باشند.(تصاویر کالای مشابه خارجی نباشد)

گذرواژه مهمترین دیوار دفاعی در برابر نفوذ به سیستم ها می باشد و امنیت آن نیز یکی از اساسی ترین مسائل در امنیت اطلاعات به شمار می رود

۱ – برای کلیه حساب های کاربری فردی(کارت بانکی، اینترنت بانک، ایمیل و...) خود یک رمز عبور یکتا و غیر تکراری استفاده نمایید.

۲ – از انتخاب گذرواژه های آسان و اصطلاحا دم دستی مانند((۱۲۳۴)(۱۱۱۱)(abcd)) خودداری نمایید .

۳ – در انتخاب گذر واژه از ترکیبی از اعداد ، سمبل و حروف لاتین استفاده نمایید مانند(bn@%۶۶۱۲)

۴ – از نوشتن گذرواژه ها بر روی کارت های بانکی خودداری نمایید.

۵ – گذرواژه های خود را با استفاده از کلمات کلیدی به صورتی انتخاب نمایید تا در ذهن شما ماندگار باشد.

هک و نفوذ

هک و نفوذ به رایانه های غیر یکی از متداول ترین جرایمی است که امروز رخ میدهد که مهمترین عامل اینگونه جرایم عدم توجه کاربران به نکات امنیتی میباشد.توجه به نکات امنیتی در هنگام استفاده از سیستم های رایانه ای ضروری می باشد

۱- از رمزهای عبور یکسان استفاده نکنید.

۲- هرگز بر روی لینک های دریافتی از سوی افراد ناشناس کلیک ننمایید.

۳- از نرم افزارهای رایگان و کرک شده تا حد امکان استفاده ننمایید.

۴-هنگام استفاده از رایانه های اماکن عمومی نکات امنیتی را بررسی نمایید و از عدم نصب نرم افزارها و سخت افزار های ثبت کلید(کی لاگر) اطمینان حاصل نمایید.

۵- به هیچ وجه از طریق ایمیل یا بستر شبکه های اجتماعی ، رمزهای عبور حساب های کاربری خود را ارسال ننمایید.

امنیت دستگاه وای فای

امروزه با یک اسکن ساده متوجه میشوید که در اطراف شما ده ها و گاها صدها دستگاه وای فای روشن باشد .اما امنیت مهمترین شرط برای استفاده از این فناوری می باشد که بدون در نظر گرفتن نکات امنیتی زیر امکان پذیر نمی باشد:

۱- در مواقع غیر ضروری و هنگام خروج از منزل دستگاه مودم خود را خاموش نمایید.

۲- سعی نمایید در اماکن عمومی از دستگاه های وای فای ناشناس استفاده ننمایید هر دستگاه وای فای ناشناس می تواند دامی از طرف سودجویان اینترنتی باشد.

۳- سعی نمایید برای انتخاب گذرواژه از ارقام و اعداد متداول (۱۲۳۴،۱۱۱۱۱و...) استفاده ننمایید و حتما از گذرواژه های ترکیبی، استفاده (اعداد، ارقام وسمبل) نمایید.

۴- به تنظیمات مودم رفته قابلیت پنهان سازی wpa/wep **را فعال نمایید.**

۵- نام کاربری و رمز عبور خود را که غالبا admin/admin **می باشد را تغییر نمایید.**

پلیس فضای تولید و تبادل اطلاعات