۲۲ نکته امنیتی ضروری در فضای مجازی

1


از اجرای ضمیمه ایمیل های دریافتی خودداری نمایید

ابزار پست الکترونیکی جهت ارسال و دریافت برنامه یا فایلهای آرشیو ایجاد نشده است. اگر فایل پیوست ایمیل، یک فایل اجرایی می‌باشد، به هیچ وجه آن را اجرا نکنید.

2


به ایمیل های ناشناس پاسخ ندهید

چنانچه ایمیلی دریافت نمودید که برای شما نا آشناست از پاسخ دادن به آن اجتناب کنید. در غیر این صورت ممکن است رخنه های امنیتی مورد نیاز هکرها را فراهم نمایید.

3


از خرید کالا به واسطه‌ی مکاتبه از طریق ایمیل خودداری نمایید

اغلب مواقع آیتمهای معرفی شده در ایمیل‌ها برای کاربران جذاب واقع می‌باشد، اما توصیه می‌گردد از خرید آنها خودداری نمایید.

4


مراقب ایمیل‌هایی که مضمون اضطراری دارند باشید

مهم نیست که این گونه ایمیل ها چقدر اضطراری و فوری هستند فقط کافیست که بدون کلیک نمودن بر روی آنها، از inbox خود حذف نمایید.

5


هیچ بانک و موسسه مالی اطلاعات مشتریان را از طریق ایمیل درخواست نمی‌کند

چنانچه ایمیلی مبنی بر تقاضای اطلاعات پرسنلی و یا کلمه عبور دریافت نمودید از پاسخ دهی به آن جدا اجتناب نمایید. چرا فکر می کنید بدون اینکه زحمتی کشیده باشید یا پروژه ای انجام داده باشید، کسی به شما پولی بفرستد؟ واقع بین باشید

6


به ایمیل هایی که اطلاعات شخصی شما را می خواهند جواب ندهید

ایمیل‌هایی که اطلاعات محرمانه (مانند شماره رمز کارت بانکی، شماره حساب و غیره) درخواست می‌نمایند بسیار خطرناک میباشند زیرا با قرار دادن اطلاعات محرمانه شما در اختیار مجرمان، زمینه را برای کلاهبرداری اینترنتی فراهم می کنند.

7


از پسوردهای پیچیده استفاده نمایید

از کلمات عبور پیچیده استفاده نمایید طوریکه توسط دیگران غیر قابل حدس باشد.

8


برای حساب های کاربری مختلف از پسوردهای مختلف استفاده کنید

هر چقدر که پسوردهای شما متنوع و مختلف باشد، شانس هک شدن حساب های کاربری شما کاهش می‌یابد.

9


از ذخیره پسوردهایتان بر روی رایانه‌ی افراد دیگر خودداری نمایید

اغلب وب سایتها هنگام Login شدن گزینه "به خاطر سپردن رمز عبور" را تدارک دیده اند، چنانچه از رایانه‌ی شخصی دیگری قصد لاگین شدن دارید ، از زدن این گزینه جدا خودداری نمایید.

10


هر نرم افزاری را روی سیستم خود نصب نکنید

برخی از وب سایتها نرم افزارهای رایگان برای کاربران نمایش میدهند، که کاربر با نصب اینگونه نرم افزارها زمینه نفوذ هکرها را فراهم می‌نماید، جهت اطمینان یافتن از این گونه نرم افزارها، به اطلاعات آن (شرکت تولید کننده محصول، وب سایت رسمی آن و غیره) توجه کنید.

11


حتما از یک آنتی ویروس کارآمد و استاندارد استفاده نمایید

با نصب آنتی ویروس تا حد قابل توجهی مانع نفوذ هکرها خواهید شد، به همین منظور آنتی ویروسهای پولی و رایگان در سطح اینترنت موجود است.
توصیه اکید می گردد حتما سیستم عامل و سایر نرم افزارهای خود را بروز نگه دارید تا حفره های امنیتی بسته شود.

12


حتما قبل از بازکردن حافظه ها آنها را اسکن کنید

قبل از باز کردن محتویات حافظه‌های قابل حمل، حتما با یک آنتی ویروس قوی آن را اسکن نمایید.

13


همیشه رایانه‌ی خود را در حالت Lock قرار دهید

به هیچ وجه رایانه‌ی شخصی خود را در حالت unlock ترک نکنید. با فعال سازی بخش پسورد گذاری سیستم عامل، می‌توانید مانع دسترسی های غیر مجاز شوید.

14


تلفن همراه خود را در حالت Auto lock قرار دهید

همیشه برروی تلفن همراه خود رمز بگذارید و مدت زمان Auto lock نباید بیشتر از یک دقیقه باشد. به این ترتیب، سارقان در دسترسی و استفاده از تلفن همراه شما با مشکل مواجه خواهند شد.

15


تلفنهای همراه در واقع نوعی رایانه‌های قدرتمند هستند، پس زیرکانه از آنها استفاده کنید

تلفنهای همراه در واقع رایانه‌های کوچکی هستند که قابلیت برقراری ارتباط با سایر وسایل الکترونیکی را داشته و حتی توانایی ذخیره سازی اطلاعات چند رسانه ای را نیز دارند.از تامین امنیت آن اطمینان حاصل کنید.

16


در شبکه های اجتماعی هرگز کسی دلش برای شما تنگ نمی‌شود

ایمیل‌هایی که با این مضمون هستند نوعی هرز نامه بوده و باید بلافاصله حذف شوند. ضمنا باید توجه داشت که اگر ایمیل به زبان انگلیسی دریافت می کنید خیلی مراقب باشید چرا که اصولا دوستان شما به فارسی ایمیل ارسال می کنند.

17


در مقابل بنرهای تبلیغاتی هوشمند باشید

به یاد داشته باشید که بنرهای تبلیغاتی که حاوی متن " شما از بین هزاران نفر برنده شده اید" یک دروغ بزرگ بوده و از کلیک نمودن بر روی آنها بایستی اجتناب کرد.

18


در هنگام پرداخت های اینترنتی به https توجه کنید

هنگام انجام تراکنش‌های بانکی ، توجه کنید که آدرس وب سایت پرداخت بانکی، بر اساس پروتکل https باشد، زیرا هنگام انجام تراکنش، اطلاعات مالی شما به صورت رمزنگاری شده تبادل خواهد شد.

19


در حد امکان از صفحه کلید مجازی استفاده کنید

در انجام تراکنش‌های بانکی از صفحه کلید مجازی که ارقام آن به صورت نا مرتب درج شده است استفاده نموده تا اطلاعات مالی شما از نرم افزارهای key logger در امان بماند.

20


اینترنت هیچ وقت دچار فراموشی نمی‌شود

چنان چه تمام اطلاعات و فایلهای خود را از اینترنت حذف نمایید یقین داشته باشید که یک نسخه از آنها در سرور دیگری ذخیره شده است.

21


از سیستم ضد هرزنامه قدرتمند استفاده کنید

با توجه به اینکه ایمیل یک روش بسیار ساده برای ارسال ویروس و بدافزار می باشد، در شبکه سازمانی، از یک ایمیل سرور مجهز به ضد ویروس و ضد هرزنامه موثر استفاده کنید.

22


از اطلاعات خود بکاپ (پشتیبان) بگیرید

آخرین و مهمترین نکته، تهیه بکاپ از اطلاعات مهم شخصی و سازمانی به صورت منظم است.
قانون مورفی را در بدبینانه ترین حالت آن در نظر بگیرید و همیشه آماده مقابله با بحران و عبور از آن باشید.