

8 راه گریز از تبهکاران اینترنتی

طبق آخرین آمارهای اعلام شده از موسسات جهانی بیش از 90 درصد پیام هایی که وارد پست الکترونیک کاربران می شود را هرزنامه ها تشکیل می دهند که تنها راه مقابله با این مسئله توجه به هشدارهای امنیتی متخصصان آگاه به امنیت اطلاعات و فرهنگسازی در این زمینه است...



طبق آخرین آمارهای اعلام شده از موسسات جهانی بیش از 90 درصد پیام هایی که وارد پست الکترونیک کاربران می شود را هرزنامه ها تشکیل می دهند که تنها راه مقابله با این مسئله توجه به هشدارهای امنیتی متخصصان آگاه به امنیت اطلاعات و فرهنگسازی در این زمینه است.

به گزارش مهر، امروزه هرزنامه (اسپم) به پدیده ای بحرانی در دنیای اینترنت و کاربران شبکه تبدیل شده که در کشور ما با توجه به جدید بودن بحث جرائم رایانه ای، این هرزنامه ها نادیده گرفته می شود و کاربران توجه زیادی به آن ندارند.

پیشرفت چشمگیر هکرها و جاسوسان الکترونیک، امنیت رایانه ها، شبکه های رایانه ای و حتی اطلاعات محرمانه اشخاص و سازمانها را به مخاطره انداخته به طوری که گفته می شود در ایران به دلیل عدم آشنایی و نبود آموزش های مدون 50 تا 60 درصد سیستم ها در خطر جاسوسی الکترونیک هستند.

آمارها نشان می دهد تبهکاران سایبری ماهانه به میلیونها رایانه در سراسر جهان حمله می کنند و تقریباً 10 درصد از آنها را آلوده می کنند.

تبهکاران سایبری به شدت در حال استفاده از بسته های ابرازی هستند که با هدف آلوده کردن رایانه های شخصی ساخته شده اند و از این رو می توانند اطلاعاتی که به صورت غیرقانونی به دست آمده را خریداری کرده و یا به فروش برسانند.

هکرها با هدف سوء استفاده های غیراخلاقی و تهدید کاربران به افشای اطلاعات محرمانه نسبت به سرقت این اطلاعات اقدام می کنند که نمونه این موضوع به وفور در کشور ما مشاهده می شود.

کارشناسان معتقدند که در ایران به دلیل عدم آشنایی با برخی ابزارها و روشهای هک و جاسوسی الکترونیک و نحوه مقابله با آن، آسیب پذیری سیستم های اطلاعاتی به مراتب بیش از دیگر کشورها است و همین امر لزوم فرهنگسازی درباره مقابله با نحوه دسترسی هکرها و جاسوسان الکترونیک به محتوای ایمیل ها، چت ها، نام های کاربری، کلمات عبور، وب سایت های مشاهده شده و شنود اطلاعات در شبکه های رایانه ای را در بردارد.

رعایت چندین نکته در مقابله با ایمیل های مخرب

رعایت چندین نکته از سوی کاربران اینترنت در هنگام کار با پست الکترونیک برای جلوگیری از آسیب های احتمالی در فضای مجازی ضروری به نظر می رسد:

1- کاربران باید از باز کردن فایل های ارسال شده (attachment) توسط ایمیل های ناشناس خودداری کنند زیرا ممکن است فایل ها حاوی برنامه های مخرب جهت سرقت اطلاعات شخصی یا از کار انداختن رایانه آنها باشد.

2- بهترین راه برخورد با نامه های الکترونیک ناشناس حذف نامه ها و پیوست آنها است.

3- اگر کاربران پیام الکترونیکی از دوست یا همکار خود دریافت کردند که در بازکردن ضمیمه فایل تاکید دارد حتماً قبل از باز کردن ضمیمه با فرستنده آن هماهنگی صورت گیرد.

4- کاربران باید از ذخیره کردن گذر واژه پست الکترونیکی خود خودداری کنند.

5- از باز کردن نامه های پست الکترونیک با عناوین نامشروع خودداری و سعی کنند از دادن اطلاعات شخصی و عضویت در این نوع گروه ها اجتناب کنند.

6- در اینترنت (فضای مجازی) سایت هایی هستند که با عضویت در آن تعدادی نامه الکترونیکی شخصی را به فرد عضو شده می فرستد که فرد با باز کردن آن نامه های الکترونیک که حاوی پیغام های تبلیغاتی است و در ازای خواندن آن مبلغی از پنج سنت تا دو دلار در یک حساب تجاری که خود شرکت معرفی کرده واریز می کنند، اما هویت و چگونگی برداشت از حساب معرفی شده دارای وجود خارجی نیست. لذا نتیجه کار تنها اتلاف وقت کاربران و صرف هزینه های مربوط به اتصال اینترنت است.

7- فضای مجازی اینترنت سرشار از تبلیغات فریبنده است که کاربران را به پولدار شدن از راه های جدید در پوشش عناوینی همچون بازاریابی شبکه ای و تجارت الکترونیک وسوسه می کند که بسیاری از این تبلیغات که از طریق ایمیل کاربران ارسال می شود جنبه امنیتی داشته و سعی دارد اطلاعات شخصی کاربر را دریافت کند. بدون شک ورود کاربران به این بازی ها یک دسیسه هرمی بیش نیست که به پولدار شدن بازیگردانان منتهی می شود.

8- کاربران به نامه های الکترونیک ارسالی ناشناس که خبر برنده شدن مبالغ قابل توجهی پول را می دهند، توجه نکنند، این روش دامی برای کلاهبرداری از کاربر است.