**چگونه در برابر دزدي‌هاي آنلاين از خود محافظت كنيم؟**

آگاهي نسبت به امنيت رايانه و افزايش شناخت نسبت به تهديدات موجود اينترنتي مانند به روزرساني نرم‌افزار امري ضروري است تا احتمال هدف قرار گرفتن توسط دزدان آنلاين را به حداقل رسانده شود همچنان كه اكنون بسياري از بانك‌ها و موسسات مالي نسبت به آموزش مشتريان خود اقدام كرده‌اند.

دزدي اطلاعات شخصي اينترنتي يكي از جرايمي است كه امروزه در كشورها بويژه در آمريكا با رشد سريعي مواجه است به طوري كه آن را جزء پنج نوع كلاهبرداري طبقه‌بندي كرده‌اند كه بسيار گزارش شده است.

آمارها نشان مي‌دهد با وجود افزايش آگاهي افراد و موسسات مالي نسبت به دزدي اطلاعات شخصي، هيچ نشاني از كاهش آن وجود ندارد و سال گذشته زيان‌هاي ناشي از دزدي اطلاعات شخصي كه ۴۰ درصد از شكايت‌هاي كلاهبرداري را شامل مي‌شود، به حدود ۳۰۰ ميليون دلار رسيد.

بر اساس اين گزارش فرد كلاهبردار به اطلاعات بيشتري نسبت به آنچه كه در كارت اعتباري وجود دارد، نيازمند است و اين اطلاعات مورد نياز توسط افراد به هنگام گشت و گذارهاي توام با بي‌احتياطي در اينترنت و استفاده از رايانه‌هايي كه امنيت آن‌ها با آلوده شدن توسط ويروس‌ها از بين رفته، فراهم مي‌شود.

يكي از دلايل دزدي آنلاين اطلاعات شخصي مورد حمله‌ي فيشينگ قرار گرفتن است، يعني شكلي از دزدي اطلاعات شخصي كه استراتژي مجرمانه در آن به كار بسته مي‌شود و كارشناسان امنيتي حرفه‌يي آن را مهندسي اجتماعي مي‌نامند و بر ارسال ايميل‌هاي فريبنده و كشاندن افراد به سايت‌هاي جعلي براي دزدي اطلاعاتي نظير شماره‌ي حساب بانك يا اطلاعات كارت اعتباري مبتني است؛ اين دزدان آنلاين از تروجان‌ها براي به دست آوردن نام كاربري و رمز عبور به منظور دست‌يابي به اطلاعات مالي افراد استفاده مي‌كنند.

كارشناسان امنيتي در حالي كه بسياري به نرم‌افزارهاي آنتي‌اسپم و آنتي‌ويروس اعتماد زيادي دارند، بر اين باورند كه برنامه‌هاي امنيتي در برابر دزدان اطلاعات شخصي چندان ضد نفوذ نيستند و اين نرم افزارها بيشتر براي رفع اكثر حملات فيشينگ و تهديدات تروجان‌ها به كار مي‌روند و در صورت همراه شدن با آگاهي كاربر از تاكتيك‌هاي مهندسي اجتماعي پيشرفته، موثر واقع خواهند شد.

بنا بر اعلام ضميمه‌ي ايميل، معمول‌ترين راه انتقال برنامه‌هاي اسب تروجان است كه بايد احتياط دو گانه‌اي را در مورد آن به عمل آورد، به اين معني كه توجه داشت كه تنها با ديدن نام فرستنده نمي‌توان از بي خطر بودن ايميل و گشودن آن اطمينان حاصل كرد؛ ورم‌هاي شبكه نيز از انواع خطرناك ويروس‌ها هستند كه بدون نياز به دخالت صاحب رايانه منتشر مي‌شوند و انواع پيشرفته‌ي آن‌ها با دسترسي به آدرس‌هاي ايميل خود، بدون آگاهي صاحب ايميل به ارسال ايميل‌هاي آلوده اقدام مي‌كنند و از اين رو هرگز نبايد ايميلي را كه انتظار دريافتش را نداريم، باز كرد و براي اطمينان بايد با فرستنده‌ي آن تماس گرفت.

كارشناسان امنيتي عقيده دارند حتي اگر با اطلاع قبلي، ضميمه‌ي ايميلي دريافت مي‌شود، باز هم خالي از خطر نخواهد بود، زيرا ممكن است فرستنده، فايل آلوده‌اي را ناخواسته ارسال كند، اين امر به عهده‌ي نرم‌افزارهاي امنيتي و آنتي‌ويروس‌ها خواهد بود تا تشخيص دهند ضميمه قابل گشودن است يا نه؛ فايل‌هاي ضميمه اغلب حاوي اسناد و گرافيك‌هايي هستند كه در صورت وجود كدهاي مخرب پنهان شده در آن‌ها، كليك بر روي آن‌ها موجب فعال شدنشان خواهد شد.

پيام‌هاي مذكور در ظاهر ممكن است حاوي مطالب مفرح يا كمك خواهي باشند كه فرد را به ارسال و اشتراك پيام با دوستان خود دعوت مي‌كند اما در كنار به كار بستن احتياط فوق‌العاده در مورد ضميمه‌ها، حفاظت چند لايه رايانه ضروري است و از اين رو نبايد تنها نرم‌افزارهاي آنتي ويروس را به كار برد بلكه بايد از رايانه در برابر اسپم‌ها و spywareها حفاظت و حداقل از محصولي استفاده كرد كه حفاظت پيشرفته‌ي ايميل و اسكن ضميمه‌هاي خطرناك را در پيام‌هاي ارسالي و دريافتي ممكن مي‌سازد؛ همچنان كه اكنون شركت‌هاي معتبري

نظير مك‌آفي، بسته‌هاي امنيتي را عرضه مي‌كنند كه شامل چندين نوع برنامه‌ي مكمل حفاظتي در برابر ويروس، اسپم، ورم و حملات فيشينگ است.

كارشناسان اعلام مي‌كنند از آن جا كه اغلب نرم‌افزارهاي امنيتي پيشرفته براي تشخيص امكان آلوده شدن سيستم رايانه، عملكرد فعلي كدهاي مخرب را مورد بررسي قرار مي‌دهند، به تاخير انداختن بروزرساني اين نرم افزارها، آن‌ها را در خطر قرار مي‌دهد، همچنين آگاهي نسبت به تنظيم ويژگي بروزرساني نرم‌افزار حائز اهميت است؛ برخي ازبرنامه‌ها امكان انتخاب يك فاصله‌ي زماني ميان بروزرساني‌هاي معمولي را مي‌دهند كه در اكثر نرم افزارهاي امنيتي، يافتن اين تنظيم آسان است.

اكثر بسته‌هاي امنيتي مشهور امكان برنامه‌ريزي براي اسكن كامل سيستم را به منظور شناسايي نفوذ گران مي‌دهند، اگرچه اين اسكن زمان‌بر خواهد بود اما بايد به موقع انجام شود تا امكان تشخيص و حذف ويروس‌هاي آسيب زننده و spywareهايي كه اطلاعات شخصي را به سرقت مي‌برند را داشته باشيم؛ يكي از عملكردهاي معمول و مطمئن، اجتناب از كليك بر روي لينك‌هاي ايميل‌هاي دريافتي است، بنابراين بايد هميشه آدرس يك وب سايت را در يك صفحه‌ي جديد مرورگر باز كرد؛ اين اقدام احتياطي ما را از خطر حملات فيشينگ مصون خواهد كرد.

بر اساس اين گزارش يكي ديگر از موارد مورد احتياط استفاده از مرورگر اينترنتي مطمئن است، به عنوان مثال مرور گر IE6 مايكروسافت هدف حملات زيادي قرار گرفت زيرا هكرها با آگاهي از اين كه ۹۰ درصد كاربران اينترنتي از اين مرورگر استفاده مي‌كنند، انواع برنامه‌هاي مخرب خود را بر اساس ضعف‌هاي امنيتي اين مرورگر طراحي مي‌كردند. البته اكنون مرورگر IE 7 با ويژگي‌هاي امنيتي ارتقا يافته و ويژگي آنتي فيشينگ آن تا حدودي اين مشكل را برطرف كرده است.

در كنار استفاده از نرم‌افزارهاي امنيتي و هوشياري به هنگام انجام داد و ستدهاي تجاري آنلاين، بايد مراقب اطلاعات اعتباري خود باشيم، براي اين كار بايد از خدمات كنترل اعتبار استفاده كرد تا اطمينان حاصل كنيم هدف دزدان اطلاعات قرار نگرفته‌ايم. يك سرويس كنترل اعتبار مي‌تواند به محض مشاهده‌ي هر معامله‌ي مشكوك كه ممكن است اطلاعات اعتباري را تحت تاثير قرار دهد، اعلام مي‌كند.

**http://www.iritn.com**