دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

هرزنامه یا اسپم چیست ؟

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

ایمیل‌های تبلیغاتی ناخواسته که از آن‌ها به عنوان اسپم یا هرزنامه نام برده می‌شود، ایمیل‌هایی بیهوده و آزار دهنده هستند. گاهی اوقات اسپم‌ها شامل پیشنهادهای جعلی هستند که فقط وقت و پول شما را از بین خواهند برد. برای توقف و محدود کردن اسپم‌ها شما می‌توانید پیشنهادی را که از طریق اسپم دریافت می‌کنید، همانند یک تماس تلفنی ناخواسته و نابجا، رد کنید. هرگز وعده و وعیدهایی که از طریق اسپم و از طرف غریبه‌ها دریافت می‌کنید، باور نکنید. سعی کنید در مورد تشخیص کلاهبرداری های رایج اینترنتی بیشتر اطلاعات کسب کنید و اطلاعات خود را در زمینهٔ تشخیص کلاهبرداری های رایج اینترنتی افزایش دهید .

چگونه می‌توانیم تعداد ایمیل‌های را که به صورت اسپم دریافت می‌کنیم، کاهش دهیم؟

از یک فیلتر ایمیل استفاده کنید:

اطمینان پیدا کنید که در کامپیوتر شما ابزاری که هرزنامه‌ها را از ایمیل اصلی جدا و به پوشهٔ ایمیل‌های ناخواسته ارسال می‌کند، وجود دارد.

شما می‌توانید از دو آدرس ایمیل استفاده کنید: از اولی برای پیغام‌های خصوصی و از دومی برای خرید اینترنتی، خبرنامه‌ها، چت روم و دیگر سرویس‌های موجود، استفاده کنید. همچنین می‌توانید از یک آدرس ایمیل دیگری استفاده کنید که با آن ایمیل‌های مورد نیاز را به ایمیل دائمی و اصلی خود بفرستید تا در صورت دریافت اسپم ، آن را (بدون هیچ اثری روی آدرس ایمیل اصلی یتان)، حذف کنید.

سعی کنید، ایمیل‌هایتان را در مقابل دید عموم قرار ندهید. برای مثال در پیام‌های وبلاگ‌ها، در چت روم، شبکه‌های اجتماعی یا دیگر فضاهایی که به صورت عمومی است، آدرس ایمیل خود را در معرض نمایش نگذارید، زیرا فرستندگان اسپم، از اینترنت برای بدست آوردن ایمیل ها استفاده می‌کنند.

حتماً سیاست های حفظ حریم خصوصی و ملاحظات را چک کنید:

قبل از ارسال ایمیل به یک وب سایت، سیاست‌های حفظ حریم خصوصی آن را بررسی کنید؛ زیرا بعضی شرکت‌ها در سیاست‌های خود این اجاره را دارند تا ایمیل شما را به دیگران بفروشند. به طور قطع؛ شما تمایلی به ارسال ایمیل به سایت‌هایی که از لحاظ امنیت در سطح پایینی هستند، ندارید.

آدرس ایمیلی منحصر به فرد انتخاب کنید:

انتخاب آدرس ایمیل می‌تواند روی تعداد اسپم‌هایی که دریافت می‌کنید، اثر بگذارد. فرستندگان اسپم، روزانه میلیون‌ها اسپم را به اسامی قابل دسترس ASPها و سرویس های ایمیلی، به امید دست یافتن به آدرس ایمیلی معتبر، ارسال می‌کنند. در نتیجه به مراتب یک اسم رایج مثل علی، تعداد اسپم‌های بیشتری در مقایسه با یک اسم خاص مثل j268kj44دریافت می‌کند. به طورقطع به خاطر سپردن یک آدرس ایمیل غیر معمولی بسیار سخت‌تر است.

چگونه می‌توانیم فرستادن ایمیل اسپم، به دیگران را کاهش دهیم:

هکرها و فرستندگان اسپم در اینترنت به دنبال کامپیوترهایی با امنیت پایین هستند و زمانی- که یک کامپیوتر حفاظت نشده یافتند، سعی می‌کنند تا یک نرم افزار پنهان به نام malware روی آن نصب کنند که از طریق آن می‌توانند کنترل کامپیوتر شما را از راه دور به دست گیرند. بسیاری از این کامپیوترها به هم وصل می‌شوند تا یک) Botnet شبکه‌ای است که فرستندگان اسپم از آن برای فرستادن میلیون‌ها ایمیل در لحظه استفاده می‌کنند)، تشکیل شود. میلیون‌ها کامپیوتر خانگی بدون اینکه صاحبانشان بدانند، در Botnet مشترک هستند. در حقیقت، اغلب اسپم‌ها از این طریق فرستاده می‌شوند.

اجازه ندهید فرستندگان اسپم از کامپیوتر شما استفاه کنند:

شما می‌توانید فرصت‌هایی را که کامپیوتر شما در اختیار Botnet قرار می‌دهد، کاهش دهید:

- از برنامهٔ امنیتی مناسبی خوب برای کامپیوتری خود استفاده کنید و هنگامی که در حال انجام کار با کامپیوترتان نیستید، ارتباط کامپیوتر خود را با اینترنت قطع کنید؛ زیرا زمانی که شما به اینترنت متصل نیستید، هکرها نمی‌توانند به کامپیوتر شما نفوذ کنند.
- هنگام دانلود و یا باز کردن هر فایلی که به ایمیل شما ضمیمه شده است، دقت کنید: هرگز ضمیمه ایمیل‌ها را باز نکنید؛ حتی اگر فکر می‌کنید از طرف یک دوست یا همکارتان فرستاده شده است،مگر اینکه شما منتظر آن هستید یا می‌دانید این فایل ضمیمه از کجا آمده و حاوی چه مضمونی است. هنگامی که در حال ارسال یک ایمیل با یک فایل ضمیمه شده به آن هستید، یک پیغام همراه با آن ارسال کنید و در آن توضیح دهید این فایل، ضمیمه شده، چیست.
- نرم افزارهای رایگان را فقط از سایت‌هایی که می‌شناسید و به آن‌ها اعتماد دارید، دانلود کنید.

گاهی ممکن است به نظر برسد، شما در حال دانلود یک برنامهٔ رایگان یا یک بازی یا یک فایل به اشتراک گذاشته شده هستید؛ اما به خاطر بسپارید که ممکن است، این نرم افزار رایگان، نرم افزار های مخرب را شامل می شود(malware)

(Malware) نرم افزار های مخرب را ردیابی و آن‌ها را حذف کنید:

درک اینکه فرستندگان اسپم ، malware روی کامپیوتر شما نصب کرده‌اند یا خیر ،کار مشکلی است؛ اما نشانه‌های هشدار دهنده ای در این رابطه وجود دارد:

♦ ممکن است؛ دوستانتان دربارهٔ ایمیل عجیبی که از جانب شما فرستاده شده است، با شما صحبت کنند.

♦ ممکن است؛ سرعت پردازش کامپیوترتان بسیار پایین آید.

♦ ممکن است در جعبه ارسال (sent items) کامپیوتر خود ایمیل‌هایی ببینند که شما آن را ارسال نکرده‌اید.

اگر کامپیوتر شما مورد هک قرار گرفت یا ویروسی شد، به سرعت اینترنت خود را قطع کنید، سپس مراحل حذف malware را انجام دهید.

منبع: ایران هشدار