



به نام خدا

نکته بسیار مهم: به هیچ عنوان و تحت هیچ شرایطی پسورد ایمیل خود را به هیچ ارگان یا نهادی ارسال نکنید. اگر ایمیلی دریافت کردید مبنی بر اینکه به دلایلی مدیر سیستم نیاز به داشتن پسورد یا اطلاعاتی از نام کاربری شما می باشد، یقین نموده که این ایمیل spam بوده و به هیچ عنوان نه اطلاعاتی به آن ارسال نموده و نه برای شخص دیگری آنرا منتشر نمایید. بهترین کار در این مواقع، حذف فوری ایمیل مشکوک از mailbox تان است.

نکاتی چند در رابطه با نامه های الکترونیکی ناخواسته و مزاحم (spam):

اولین مسئله این است که چگونه آدرس ایمیل افراد بدست ارسال کننده های spam می رسد. Spammer ها از روشهای مختلفی به آدرس ایمیل افراد دسترسی پیدا می کنند:

۱. از mailing list ها. بدین صورت که با ترفندهای مخصوص، لیست ایمیل های مشترکین mailing list ها را به دست می آورند.
۲. از طریق صفحات وب. چه صفحات عمومی سرورهای وب مثل صفحات وب دانشگاه و چه وب سایت شخصی خود کاربران.
۳. از طریق صفحات و فرم های اینترنتی که در آنها ثبت نام می دهید. بعضی از سایتها از شما اطلاعاتی جهت ثبت نام، خرید اینترنتی و ... تقاضا می کنند که یکی از این اطلاعات، آدرس ایمیل است. آدرسی که در این فرمها می نویسید توسط spammer ها به راحتی قابل دستیابی است.
۴. از طریق address book افراد. بدین صورت که اگر spammer آدرس شخصی را بدست آورده باشد می تواند بصورت اتوماتیک به تمام آدرس های موجود در address book وی دست یافته و آنها را نیز ویروسی کند.



- همچنین بعضی موتورهای جستجو قادرند آدرسهای ایمیل را از قسمت: To ، BCC: و CC: ایمیلهای رد و بدل شده استخراج کنند.
۵. خرید لیست ایمیل اشخاص از دیگران.
۶. از طریق پنجره های pop up. زمانی که وارد سایتی می شوید و بطور اتوماتیک یک پنجره جدید باز می شود که منوی YES و NO دارد که ممکن است هر کدام از آنها حتی NO را هم کلیک نمایید باز هم اطلاعاتی از کامپیوتر شما به آن سرور فرستاده شود.

اقداماتی که کاربران سیستم برای جلوگیری از انتشار ویروس ها و اسپمها باید انجام دهند:

۱- هرگز آدرس ایمیل خود را در صفحات عمومی و صفحه پیغام رسانی وب سایتتان قرار ندهید به عنوان مثال، اگر آدرس شما بصورت `user@kntu.university` می باشد، آن را بصورت `user{AT}kntu[dot]university` یا هر روش دلخواه دیگری بنویسید.

۲- اگر برای گرفتن اطلاعات به سایتی سر می زنید که شما را مجبور می کند آدرس ایمیل خود را وارد کنید، هیچگاه از آدرس ایمیل آکادمیک و دانشگاهی استفاده نکنید. به جای آن می توانید از آدرس ایمیل یاهو یا جی میل و ... استفاده کنید.

۳- حتی المقدور روی لینک یا آدرسی که خروج شما را از فهرست گیرندگان spam و یا قطع اشتراک پیشنهاد می دهد کلیک ننمایید زیرا به آنها اطلاع می دهد که نامه آنها را دریافت کرده اید و آدرس شما فعال است و این کار باعث می شود که spam های بیشتری نیز دریافت نمایید.



۴- هیچگاه به ایمیل‌های مشکوک پاسخ نداده و آن را برای کسی forward نکنید. بهترین کار این است که آنها را از mailbox تان پاک کنید.

۵- اگر برای ثبت فرم اینترنتی آدرس ایمیلی از شما خواسته شد، آدرس ایمیل دانشگاه را وارد نکنید. همچنین کلمه رمز عبوری (password) که برای استفاده از ایمیل دانشگاه به کار می‌برید را برای کاربردهای دیگر استفاده نکرده و آن را در جای دیگری غیر از صفحه اصلی ایمیل دانشگاه وارد نکنید. اگر برای تکمیل فرم ثبت نام از شما کلمه عبور خواسته شد، حتما کلمه عبور دیگری غیر از پسورد ایمیلتان برگزینید.

۶- با آدرس ایمیل دانشگاه عضو لیست های مختلف اینترنتی و ایمیلی نشوید.

۷- کلمات عبور مطمئن و ایمن برای خود انتخاب کنید. یک پسورد خوب و مطمئن باید حداقل شامل ۶ کاراکتر ترکیبی از حروف و اعداد و علامات مخصوص باشد و همچنین قابل حدس زدن نیز نباشد. پسورد هایی مثل نام و نام خانوادگی تان، ۱۱۱۱۱۱، ۱۲۳۴۵۶ و از این قبیل، بدترین انتخاب برای شماست. **هیچگاه از همان کلمه نام کاربری خود، جهت رمز عبور استفاده نکنید.**

۸- از پسورد خود مراقبت کرده و آن را در اختیار دیگری قرار ندهید. اگر زمانی مجبور به این کار شدید در اولین فرصت، آن را تغییر دهید.

۹- از دستگاہی که برای چک کردن ایمیل‌های دانشگاه استفاده می‌کنید به خوبی مراقبت کرده، آن را در اختیار افراد ناشناس و غیر اخلاقی نگذاشته و از طریق آن به سایتهای مشکوک وارد نشوید.



۱۰- سیستم عامل (ویندوز) و نرم افزارهای روی دستگاهتان را همواره به روز نگه داشته و آنتی ویروس آن را همیشه update نگه دارید.

اقداماتی که دانشگاه در این زمینه انجام داده است:

در ابتدا سعی شده است در سایتهای عمومی، آدرس ایمیل ها به شکلی نوشته شود که آدرس ایمیل برای خواننده مفهوم بوده ولی نرم افزارهای مربوطه نتوانند برای سوء استفاده دریافت نمایند (در سایتهای شخصی، خود اساتید محترم باید این کار را انجام دهند). همچنین نرم افزارهای آنتی ویروس و آنتی اسپم مطمئن خریداری شده و همواره به روز نگه داشته می شوند.

این تدابیر تا حدود زیادی از ورود spam به آدرس ایمیل کاربران جلوگیری می کند. حال این سوال مطرح می شود که با وجود این برنامه های تشخیص و پیش گیری، چرا کاربران هنوز هم گاهی spam هایی دریافت می کنند؟

در پاسخ می توان گفت که حجم spam هایی که وارد دانشگاه می شوند و سیستم بطور اتوماتیک جلو آنها را می گیرد بسیار بالا بوده و سیستم پس از شناسایی، مانع از ورود آنها به شناسه کاربران می گردد. در واقع spam های دریافتی توسط کاربران سهم بسیار کمی از کل spam های واقعی است که به شناسه آنها می آید بقیه آنها توسط سیستم از بین خواهند رفت. بطور معمول هر شخصی که از اینترنت و ایمیل بیشتر استفاده می کند spam بیشتری هم دریافت می نماید.

آنچه که مسلم است، برنامه های تشخیص spam موجود نمی توانند مانند انسان متن موجود در ایمیل را تشخیص داده و از spam بودن آن مطلع گردند. این نرم افزار ها یک سری پارامترهایی برای تشخیص spam دارند. با استفاده از این پارامترها توسط برنامه آنتی ویروس و آنتی اسپم، یک نمره یا امتیاز برای آنها در نظر گرفته می شود. مثلا اگر در ایمیل ای دو پارامتر صدق کند درجه امتیاز آن دو می شود. حال اگر امتیاز مربوط به یک ایمیل کم باشد آن ایمیل به دست



شما می‌رسد ولی در ابتدای موضوع (subject) آن ایمیل عبارت {spam} اضافه می‌گردد. وقتی امتیاز آن از یک حدی که در برنامه مشخص می‌کنیم بیشتر شود آن ایمیل بدست شما نمی‌رسد و به عنوان یک ایمیل spam حذف می‌گردد.

نکته مهم اینجاست که هر چه حد بالایی امتیاز را کم کنیم شما spam کمتری دریافت می‌کنید ولی در عوض احتمال اینکه ایمیل واقعی را از دست بدهید بیشتر است؛ کما اینکه گاهی شما ایمیلی دریافت نموده اید که در subject آن عبارت spam وجود داشته ولی آن ایمیلی واقعی بوده است.

سؤال دیگری که مطرح است این که چرا ایمیل‌های دانشگاهی spam بیشتری دریافت می‌کنند؟ به این علت که ایمیل‌های موجود در yahoo مانند ایمیل‌های دانشگاه در وب‌سایت‌های عمومی دانشگاه و وب‌سایت شخصی افراد موجود نمی‌باشد و به همین علت بسیاری حاضرند آدرس ایمیل‌های دانشگاهی و موسسات را برای ارسال تبلیغ استفاده نمایند و اینکه اعتبار ایمیل‌های دانشگاهی و موسسات به دلیل نوع فعالیت آنها خیلی بیشتر از ایمیل‌های yahoo و ... می‌باشد.

ترفند جدیدی که spammerها از آن استفاده می‌کنند فرستادن spam به نام خود شخص است که کار فیلترینگ را مشکلتر می‌کند. این spammerها مطمئن هستند که از طریق نام فرستنده نمی‌توانیم این نوع ایمیل‌ها را فیلتر نماییم و این در برنامه موجب پایین آمدن score ای که در بالا ذکر شد می‌گردد.

موفق باشید

دفتر فناوری اطلاعات دانشگاه