پیش از کلیک کردن برروی این پیوند‌های کوتاه شده از خود این ۵ سؤال را بپرسید …

امروزه URLها راه آسان و خوبی برای رسیدن به مقصد اینترنتی به جای وارد کردن آدرس کامل است، اما با وجود جرایم اینترنتی پیشرفته باید مراقب حملات بود چرا که می‌توانند منجر به سرقت گذرواژه‌ها یا داده‌ها شوند.بنابراین پیش از کلیک کردن برروی این پیوند‌های کوتاه شده از خود این ۵ سؤال را بپرسید:

**۱- آیا به کسی که پیوند را برای شما ارسال کرده‌ اعتماد دارید؟**

اعتماد در دنیای برخط باید به همان صورتی باشد که در دنیای واقعی از آن یاد می‌کنیم، اما متأسفانه به ندرت این اتفاق می‌افتد. برای مثال، مردم قبل از باز کردن در اصلی خانه معمولاً چشمی در را اول بررسی می‌کنند و به فرزندانشان گوشزد می‌کنند که مراقب غریبه‌ها باشند، اما همین مردم ممکن است رایانامه یا پیوند ارسالی از طرف یک ناشناس را باز کنند.

خبر خوب آن است که، علی‌رغم این که فیشینگ هنوز هم یک ابزار محبوب برای مجرمین اینترنتی است، قدرت تشخیص مردم نیز برای تمایز بین رایانامه‌های (و پیوند‌های) خوب و بد زیاد شده است. این مهم با کمک پالایش هرزنامه بهتر هم شده است.

اولین سؤالی که باید از خودتان بپرسید این است که آیا به کسی که پیوند را فرستاده یا به اشتراک گذاشته است اعتماد دارم؟ اگر پیوند توسط یکی از اعضای خانواده یا یک دوست و یا شبکه‌ی معتمد فرستاده شده بود مشکلی نیست، اما اگر به هردلیلی درباره‌ی فرستنده‌ی آن مطمئن نیستید می‌توانید با فرستنده تماس بگیرید و از صحت ارسال از طرف او مطمئن شوید.

اما اگر فرستنده، یا آدرس رایانامه و یا محتوای رایانامه را نمی‌شناسید بهترین گزینه این است که آن را باز نکنید. به خصوص باید در مواردی که در عنوان رایانامه نام شما ذکر شده یا مدعی شده است که از طرف بانک شما است جوانب احتیاط را رعایت کنید.

**۲- آیا به بستر نرم‌افزاری مورد علاقه‌تان اعتماد دارید؟**

مانند سایر سؤالات مطرح شده در این فهرست، این سؤال هم مهم است. برای مثال اگر پیوندی از طریق شبکه‌ی داخلی کاری‌تان و یا گروه خصوصی واتس‌اپ به اشتراک گذاشته شده است جای نگرانی وجود ندارد، اما اگر پیوندی در هرزنامه باشد یا از سوی حساب کاربری ناشناسی در توئیتر فرستاده شده باشد، باید قبل از کلیک کردن روی آن بیشتر فکر کنید.



درمورد توئیتر و فیس‌بوک بیشتر مراقب باشید. در هردوی آن‌ها هرزنامه‌هایی گزارش شده است که حاوی پیوند‌هایی بوده‌اند که مستقیماً شما را به وب‌گاه‌های مخرب هدایت می‌کنند. به علاوه در این شبکه‌های اجتماعی حساب‌های کاربری متعددی نیز مورد نفوذ واقع شده است.

**۳- آیا به مقصدی که پیوند شما را هدایت خواهد کرد اعتماد دارید؟**

به پیوندی که به اشتراک گذاشته شده است نگاه کنید، آیا شما را به وب‌گاهی هدایت می‌کند که می‌شناسید؟

اگر به مقصد آن اعتماد ندارید یا آن را نمی‌شناسید نباید روی آن کلیک کنید. به‌جای آن، خودتان به طورمستقیم آدرس مقصد اینترنتی مدنظرتان را جست‌وجو کنید.

**۴- آیا این پیوند متقارن با زمان وقوع رویدادی جهانی است؟**

مجرمان اینترنتی بسیار فرصت طلب‌اند. آن‌ها از هر فرصتی برای به دام انداختن افراد برای کلیک کردن روی پیوند‌هایشان استفاده می‌کنند، مخصوصاً زمانی که نزدیک یک رویداد بزرگ مانند المپیک، جام جهانی هستیم و یا به هنگام رخداد فجایع،تعداد هرزنامه‌ها و توئیت‌ها در این مواقع به سرعت زیاد می‌شود.



بنابراین اگر پیوندی دیدید، مثلاً درباره‌ی زلزله‌ی نپال، درباره‌ی آن خوب فکر کنید تا بتوانید به سؤال‌های قبل پاسخ دهید، این که چه کسی آن را به اشتراک گذاشته است، منبع آن کجاست و به چه مقصدی شما را هدایت خواهد کرد.

**۵- آیا پیوند دریافتی، یک پیوند کوتاه‌ شده است؟**

گسترش شبکه‌های اجتماعی هم‌چون فیس‌بوک، توئیتر و اینستاگرام نیاز را به پیوند‌های کوتاه‌شده افزایش داده‌اند. برخی از این پیوند‌ها در کمین شما هستند.

برای مثال، یک مجرم اینترنتی می‌تواند پیوند مخرب خود را از طریق وب‌گاه‌هایی مانند Bitly، goo.gl و… کوتاه کند به امید این‌که شما به آن به عنوان یک منبع مورد اعتماد نگاه کنید. به خصوص اگر او پیوند خود را با توئیت یا پیوند معتبری ترکیب کند، کاربر به سمت باور اینکه پیوند مورد اعتماد است تشویق خواهد شد.

بنابراین برای پیوند‌های کوتاه شده، ابتدا پاسخ سؤال‌های قبلی را برای خود بیابید. هم‌چنین می‌توانید از ابزارهایی مانندLongURL و یا CheckShortURL برای بازگرداندن پیوند کوتاه‌شده به حالت معمولی استفاده کنید.

منبع:

[آی تی اس ان (پایگاه خبری امنیت فناوری اطلاعات](http://www.itsn.ir/)