امنیت پست الکترونیک

شش نکته مهم امنیت ایمیل که باید بدانید

تمرین ها و تجربه های آنلاین ایمن در حفظ صد در صد هویت آنلاین شما و رهایی از ویروس ها، هکرها و همه گونه حقه ها و شیطنت های مبتنی بر اینترنت، ارزشمند هستند. و بهترین مکان برای شروع کجاست؟ صندوق پستی‌تان. در اینجا برخی نکات ساده اما مهم امنیتی آمده است که تا آنجا که امکان دارد باید برای حفظ امنیت حساب ایمیل خود بدانید.

۱. از حساب های ایمیل جداگانه استفاده کنید.

اگر شما همانند بیشتر مردم هستید، حساب ایمیل تان احتمالا قطب مرکزی فعالیت های شخصی شماست. همه اطلاعیه های فیس بوک، ثبت نام های وبگاه، خبرنامه ها، پیام های شما، و غیره به ایمیل تان فرستاده می شوند، درست است؟ این بدان معنا است که شما همه تخم مرغ هایتان را در یک سبد می گذارید، اگر آن سبد اتفاقی سقوط کند، شما همه تخم مرغ هایتان را با آن از دست خواهید داد. داشتن حساب‌های ایمیل جداگانه نه تنها به افزایش امنیت شما کمک خواهد کرد، بلکه همچنین به ارتقا بهره وری شما می‌انجامد. تصور کنید اگر بتوانید تمامی ایمیل های کاری خود را در یک حساب کاری ادغام کنید؛ تمامی دوستان و خانواده با حساب شخصی تان مکاتبه می‌کنند؛ دارای یک حساب تفننی برای وبگاه ها هستید؛ و یک حساب دم دستی برای لینک های هرزنامه ای ناشناخته دارید. به این ترتیب، اگر کسی حساب کاری تان را هک کند، تمام ایمیل های شخصی تان هنوز در امان هستند.

۲. یک گذرواژه منحصر به فرد ایجاد کنید.

همراه با اندیشه چندین حساب، می بایست همچنین یک گذرواژه (رمز عبور) کاملا یکتا و منحصر به فرد برای هر یک از حساب‌های ایمیل خود داشته باشید. حتی اگر تصمیم به نگهداشتن یک حساب ایمیل اصلی دارید، مطمئن شوید که گذرواژه آن ٪۱۰۰ منحصر به فرد است. استفاده از یک گذرواژه برای همه حساب‌های‌تان، اشتباهی در سطح افراد تازه کار است. فرض کنید کسانی ایمیل شخصی‌تان را هک کنند پس تمامی اطلاعیه‌های دریافتی فیس‌بوک، پیام‌های کاری و غیره را مشاهده می‌کنند. هر هکر ابلهی آن حساب‌ها را با گذرواژه‌های یکسان به عنوان حساب ایمیل‌تان آزمایش خواهد کرد، و در مورد شما آنها موفق خواهند شد.

۳. هرگز روی لینک ها در ایمیل ها کلیک نکنید.

هر زمان که لینکی (پیوند) را در یک ایمیل می بیند، در ٪۹۹ اوقات نباید روی آن کلیک کنید. تنها موارد استثنایی هنگامی است که شما در انتظار ایمیل خاصی هستید، همچون لینک ثبت نام یک انجمن یا ایمیل فعال سازی حساب کاربری بازی، یا چیزهایی همانند این. اگر شما یک ایمیل هرزنامه که تلاش می کند تا خدمات یا محصول خاصی را به شما بفروشد، دریافت می کنید، هرگز بر روی هیچ یک از لینک های درون آن کلیک نکنیدگاهی اوقات آنها ممکن است امن باشند؛ اوقاتی دیگر آنها شما را مستقیم به سوی درهای جهنم می برند و با انبوهی از نرم افزارهای مخرب و ویروس ها مواجه می کنند. اگر شما ایمیلی از بانک خود یا هر خدمات دیگری (به عنوان مثال، پرداخت صورت حساب یا قبض) دریافت نمودید، همیشه به صورت دستی از وبگاه بازدید کنید. بدون کپی کردن و چسباندن (paste). بدون کلیک مستقیم. بعدها از خود سپاسگذاری خواهید کرد.

٤. پیوست‌های ناخواسته را باز نکنید.

پیوست ها هنگامی که به ایمیل می آیند، چیزهای فریبنده ای هستند. اگر شما در انتظار چیزی از طرف یک دوست یا همکار هستید، پس با اطمینان، دست به کار شوید و پیوست را باز کنید. اما در صورتی که ایمیل ناخواسته‌ای است، هرگز هیچ فایل پیوستی را باز نکنید. حتی اگر فایل سالم و بی‌ضرر به نظر برسد، شما ممکن است با جهانی از آزار و ناراحتی روبرو شوید. با دانلود کردن و بازکردن پیوست‌های ناخواسته ممکن است سیستم شما به راحتی آلوده به بدافزار شود.

٥. ویروس‌ها و نرم افزارهای مخرب را اسکن کنید.

اگر ایمیلی را باز می کنید و به هر حال مشکوک به نظر می‌رسد، دست به کار شوید و یک اسکن کننده نرم‌افزارهای مخرب و ویروس را اجرا کنید. هر ایمیل هرزنامه‌ای شما را به ویروس آلوده نخواهد کرد و این ممکن است زیاده روی به نظر برسد که هر زمان یک ایمیل مشکوک را باز می کنید، اسکن کننده نرم افزار های مخرب را اجرا نمایید، اما در امان بودن بهتر از تأسف خوردن است.

٦. از وای–فای عمومی پرهیز کنید.

هنگامی که در اینترنت عمومی هستید از بررسی ایمیل خود پرهیز کنید. متاسفانه، وای‌فای عمومی می‌تواند بسیار نا امن باشد. برنامه‌هایی وجود دارند که بی تحرک در پس زمینه دستگاه برخی هکرها اجرا می شوند. این برنامه‌ها تمامی داده‌های بی‌سیم جاری در سراسر یک شبکه خاص را زیر نظر می‌گیرد، و آن داده‌ها ممکن است برای اطلاعات مهمی مورد تجزیه و تحلیل قرار گیرند. همانند نام کاربری و گذرواژه شما.

امنیت ایمیل به عقل سلیم و تصمیم های دقیق منحصر می شود. اجازه ندهید تنبلی و آسایش بر آرزو و خواست شما برای محافظت و آرامش سایه افکند.