

OUCH!

ماهنامه نگاهی از امنیت اطلاعات برای شما

از رایج ترین اشتباهات مربوط به ایمیل اجتناب کنید

ایمیل هنوز یکی از راههای اصلی ارتباطی ما، هم در زندگی شخصی و هم در زندگی حرفه ای است. با این حال، اغلب هنگام استفاده از ایمیل می توانیم بدترین دشمن خودمان باشیم. در اینجا رایج ترین اشتباهاتی که افراد هنگام استفاده از ایمیل مرتکب می شوند و راه های جلوگیری از آنها را توضیح خواهیم داد.

تکمیل خودکار

تکمیل خودکار یک ویژگی رایج در اکثر سرویس گیرندگان ایمیل (کلاینت ها) است. با تایپ کردن نام شخصی که می خواهید برایش ایمیل ارسال کنید، نرم افزار ایمیل شما به طور خودکار آدرس ایمیل وی را برای شما انتخاب می کند. به این ترتیب نیازی نیست آدرس ایمیل همه مخاطبین خود را به خاطر بسپارید و فقط دانستن نام آنها کافی است. مشکل وقتی پیش می آید که افرادی را با نام های مشابه هم می شناسید، انتخاب آدرس ایمیل اشتباه برای قابلیت تکمیل خودکار بسیار آسان خواهد بود. به عنوان مثال، ممکن است شما قصد ارسال یک ایمیل کاری بسیار حساس به "Janet Roberts"، همکار خود را داشته باشید، اما در عوض قابلیت تکمیل خودکار آدرس ایمیل "Janice Rodriguez"، مربی بسکتبال فرزند شما را انتخاب می کند. در نهایت یک ایمیل کاری حساس برای شخصی که تقریباً نمی شناسید ارسال می کنید. همیشه در زمان ارسال هر ایمیل حساسی، نام و آدرس ایمیل را قبل از اینکه دکمه ارسال را بزنید دوباره چک کنید. گزینه دیگر این است که ایمیل گیرنده را بعد از تهیه و تکمیل پیام خود اضافه نمائید تا اطمینان حاصل کنید که فرد مورد نظر را درست انتخاب کرده اید.

پاسخ-به همه (Reply-All)

علاوه بر قسمت "To" هنگام ایجاد یک ایمیل، یک گزینه "CC": نیز دارید. گزینه "CC": مخفف "Carbon Copy" است که به شما امکان می دهد افراد دیگری را در ایمیل خود کپی کرده و آنها را مطلع سازید. وقتی شخص دیگری برای شما ایمیلی ارسال می کند و افرادی را در "CC" خود قرار داده است، باید تصمیم بگیرید که چگونه می خواهید پاسخ دهید: فقط به ارسال کننده، یا از طریق Reply-All به همه کسانی که در ایمیل موجود میباشند پاسخ دهید. اگر پاسخ شما حساس است، به احتمال زیاد می خواهید فقط به فرستنده ایمیل پاسخ دهید. با این حال، مراقب باشید زیرا به سادگی می توانید "Reply-All" را بزنید، به این معنی که به همه افراد موجود در ایمیل پاسخ می دهید. یکبار دیگر یادآوری میکنیم، زمانیکه به یک ایمیل حساس پاسخ میدهید، همیشه دوباره بررسی نمائید که ایمیل را به چه کسی میفرستید قبل از اینکه دکمه ارسال را فشار دهید.

احساسات

هرگز زمانیکه از لحاظ احساسی ناراحت هستید ایمیلی ارسال نکنید--این مسئله ممکن است در آینده به شما آسیب برساند، حتی شاید هزینه اش نابودی دوستی و یا شغل شما باشد. در عوض، یک لحظه وقت بگذارید و با آرامش افکار خود را سازماندهی کنید. اگر نیاز دارید ناراحتی خود را تخلیه کنید، یک ایمیل جدید باز کنید (مطمئن شوید که در قسمت "TO" هیچ نام یا نشانی ایمیلی وجود ندارد) و دقیقاً آنچه را که می خواهید بگویید تایپ کنید. سپس برخیزید و از رایانه خود دور شوید، شاید بهتر است برای خود یک فنجان قهوه درست کنید یا قدم بزنید. وقتی برگشتید، پیام خود را پاک کرده و دوباره از اول شروع کنید. حتی ممکن است داشتن یک دوست یا همکار جهت بررسی بی طرف پیش نویس ایمیل شما قبل از ارسال آن، کمک شایانی باشد. یا شاید وقتی آرام شدید، بهتر است تلفن را بردارید و به سادگی با آن شخص صحبت کنید، یا در صورت امکان رو در رو صحبت کنید. ممکن است برای افراد سخت باشد که قصد شما را فقط با یک ایمیل متوجه شوند، بنابراین احتمال دارد پیام شما از طریق تلفن یا رو در رو بهتر به نظر برسد. به یاد داشته باشید، وقتی آن ایمیل را ارسال میکنید، برای همیشه وجود خواهد داشت.

حریم خصوصی

در نهایت، ایمیل دارای حفاظتهای محدودی از حریم خصوصی میباشد. هر کسی که به آن دسترسی پیدا کند می تواند ایمیل شما را بخواند، مانند کارت پستال ارسال شده توسط پست. ایمیل شما می تواند به راحتی به دیگران ارسال (فوروارد) شود، در انجمن های عمومی پست شود، به دلیل حکم دادگاه منتشر شود یا پس از هک شدن سرور توزیع شود. اگر واقعاً چیزی خصوصی دارید که به کسی بگویید، تلفن را برداشته و با آنها تماس بگیرید. اگر از رایانه کاری خود برای ارسال ایمیل استفاده می کنید، به یاد داشته باشید که کارفرمای شما ممکن است حق نظارت و حتی خواندن ایمیل شما را هنگام استفاده از منابع کاری داشته باشد.

پیوست ها

اگر اسنادی را به پیام خود ضمیمه می کنید، قبل از ارسال، مجدد بررسی کنید که نسخه های صحیح از فایل های صحیح را ضمیمه کرده باشید.

سردیر مهمان

Steffanie AK Schilling یک ستاره راک امنیت سایبری است که ریشه در علوم اجتماعی دارد. او به عنوان "مبتکر و تفاوت ساز در فضای مجازی" مفتخر شده است و یکی از اعضای افتتاحیه ShareTheMicInCyber است و در حال حاضر به عنوان جوانترین معاون تاریخ Infragard - شمال اوهایو خدمت می کند. او یک سخنران بسیار مورد استقبال در زمینه تنوع، برابری، شمول، عدالت و آموزش و آگاهی امنیتی است. آدرس لینکدین: (<https://www.linkedin.com/in/steffanieschilling>).

منابع

حملات مهندسی اجتماعی: <https://www.sans.org/newsletters/ouch/social-engineering-attacks>
سرقت هویت: <https://www.sans.org/newsletters/ouch/identify-theft>
شغلی در حوزه امنیت سایبری: <https://www.sans.org/newsletters/ouch/a-career-in-cybersecurity>

ترجمه شده برای عموم توسط: سعید میرجلیلی، مجید هدایتی

IOUCH توسط برنامه "زندگی امن" موسسه SANS تحت مجوز [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/) منتشر و توزیع میشود. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. هیئت تحریریه: Walter Scrivens, Phil Hoffman, Alan Waggoner, Les Ridout, Princess Young.