بایدها و نبایدهای پیام رسانی

مقدمه

پیام رسانی به عنوان یک روش اصلی ارتباط در زندگی شخصی و حرفه ای ما عمل می کند. با این حال، اغلب اوقات ما وقتی به پیام رسانی امن و ایمن میپردازیم، می‌توانیم بدترین دشمن خودمان باشیم. رایج ترین اشتباهاتی که مردم مرتکب می شوند را بیاموزید و یاد بگیرید چگونه می توانید از آنها در زندگی روزمره خود اجتناب کنید.

تکمیل خودکار(Auto-Complete)

تکمیل خودکار یک ویژگی رایج در بسیاری از برنامه‌های پیام‌رسان است. همانطور که نام شخصی را که می خواهید پیام ارسال کنید تایپ می کنید، برنامه شما ممکن است به طور خودکار فرد مورد نظر را برای شما انتخاب کند. این ویژگی می تواند منجر به اشتباهات شود، به خصوص زمانی که چندین مخاطب نام های مشابه دارند. به عنوان مثال، ممکن است قصد ارسال یک متن حساس به یک همکار را داشته باشید، اما در عوض به طور تصادفی به مربی دخترتان که نام بسیار مشابهی دارد پیام دهید. همیشه قبل از زدن دگمه ارسال، نام کامل شخصی را که می‌خواهید پیام ارسال کنید، دوباره بررسی کنید.

پاسخ به پیام های گروهی

چت های گروهی یکی دیگر از ویژگی های رایج است، اما مطمئن شوید که قبل از پاسخ دادن، از همه اعضای گروه که در لیست هستند آگاه هستید. وقتی به کل گروه پاسخ می دهید، لازم است مطمئن شوید که پاسخ شما برای همه افراد آن گروه مناسب است. یکی دیگر از اشتباهات رایج، پاسخ دادن تصادفی به کل گروه به جای یک فرد خاص است. برای پاسخ دادن وقت بگذارید: قبل از زدن دکمه ارسال، دوباره چک کنید.

احساسات

در هنگام عصبانیت، ناراحتی، یا فراوانی احساسات از ارسال پیام خودداری کنید. این پیام می‌تواند آسیب‌های بسیار بیشتری در آینده به شما وارد کند، حتی ممکن است به قیمت یک دوستی یا شغل شما تمام شود. در عوض، لحظه ای را به سازماندهی افکار خود اختصاص دهید. اگر شما *لازم است* ناراحتی خود را تخلیه کنید، پیام جدیدی را بدون هیچ گیرنده ای باز کنید، دقیقاً آنچه را که احساس شما است تایپ کنید، سپس از دستگاه خود دور شوید. شاید بهتر است برای خود یک فنجان چای درست کنید یا به پیاده روی بروید. وقتی برگشتید، پیام را حذف کنید و دوباره شروع کنید. به احتمال زیاد در وضعیت ذهنی بسیار آرام تر و واضح تری خواهید بود. برای مکالمه موثرتر ارتباط مستقیم از طریق تلفن یا حضوری را در نظر بگیرید. تعیین لحن و هدف شما فقط با یک پیام متنی ممکن است برای افراد دشوار باشد.

حریم خصوصی

پیام‌های پاس ام اس های سنتی فاقد حفاظت از حریم خصوصی قوی هستند. پس از ارسال، کنترل پیام را از دست می دهید. پیام‌ها را می‌توان به‌دلیل دستورهای دادگاه ارسال کرد، به‌صورت عمومی پست کرد، به‌صورت اسکرین‌شات به اشتراک گذاشت یا افشا کرد. برای ارتباط خصوصی، تلفن را بردارید و با فرد تماس بگیرید. در نهایت، اگر از دستگاه کاری خود برای پیام‌رسانی استفاده می کنید، به یاد داشته باشید که کارفرمای شما ممکن است اختیار نظارت و خواندن پیام‌ها را در دستگاه‌های کاری در اختیار داشته باشد.

پیام های مخرب

مانند ایمیل، مهاجمان سایبری سعی می کنند با پیام ها شما را فریب دهند، گولتان بزنند یا کلاهبرداری کنند. این پیام‌ها می‌توانند شامل پیوندهای مخربی باشند که مهاجمان می‌خواهند روی آن‌ها کلیک کنید، درخواست‌هایی از شما برای به اشتراک گذاشتن اطلاعات شخصی یا فشار برای تماس با یک شماره تلفن. آیا تا به حال یک پیام متنی عجیب و غریب با کلمه "سلام" در پیام دریافت کرده اید و فکر کرده اید که این پیام در مورد چیست؟ این یک مهاجم سایبری است که سعی می کند با شما مکالمه را آغاز کند، که اغلب شروع چیزی به نام کلاهبرداری عاشقانه است. اگر پیام‌های عجیب و غریب یا مشکوکی در دستگاه خود دریافت می کنید، به سادگی آن‌ها را حذف کنید.

علاوه بر این، همانطور که در مورد ایمیل نیز صدق میکند، می توان منبع یک پیام متنی را جعل کرد. قبل از افشای هر گونه اطلاعات شخصی، مطمئن شوید که هویت شخصی که به او پیامک می‌دهید را می‌دانید، به‌خصوص اگر شما شروع کننده مکالمه نبوده‌اید. همچنین می‌توانید شماره‌های تلفن یا حساب‌های ناخواسته یا مشکوکی را که سعی در ارسال پیام به شما دارند، مسدود کنید.

پیام رسانی ایمن

مطمئن شوید هر برنامه پیام‌رسانی که استفاده می‌کنید به‌روز و جدید باشد، مطمئن شوید که آخرین ویژگی‌های امنیتی را دارد. برای افزایش امنیت و حفظ حریم خصوصی، برنامه‌های پیام‌رسان ایمن اختصاصی مانند Signal را در نظر بگیرید.

سردبیر مهمان

میشل توماسیک، زنان در امنیت سایبری (WiCyS)، معاون مدیر، یک رهبر پویا است که متعهد به پیشرفت زنان در زمینه امنیت سایبری است. او با پیشینه ای قوی در مدیریت افراد و عملیات، از تخصص خود برای ترویج فراگیری، تنوع و توانمندسازی زنان در نیروی کار امنیت سایبری استفاده می کند.

منابع

اسفاده ایمن از دستگاههای تلفن همراه: https://www.sans.org/newsletters/ouch/securing-mobile-devices
دورانداختن دستگاههای تلفن همراه: https://www.sans.org/newsletters/ouch/disposing-mobile-devices
ممانعت از اشتباهات رایج عمومی در ایمیل: https://www.sans.org/newsletters/ouch/avoid-the-most-common-email-mistakes
سیگنال: https://signal.org

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو