نکات برتر امنیت سایبری برای تعطیلات

مقدمه

با نزدیک شدن به فصل تعطیلات، میلیون ها نفر به سفر خواهند رفت. اگر شما هم جزو این افراد هستید، در اینجا چند نکته وجود دارد که به شما کمک می‌کند تا در فضای مجازی هوشیار و ایمن باشید.

- دستگاه های تلفن همراه: تا جایی که میتوانید دستگاههای کمتری همراه خود بیاورید. هر چه دستگاه های کمتری در سفر به همراه داشته باشید،دستگاه های کمتری ممکن است گم شده یا دزدیده شود. در حقیقت، آیا می‌دانستید که احتمال گم شدن یک دستگاه تلفن همراه بیشتر از دزدیده شدن آن است؟ زمانی که اتاق هتل، رستوران، تاکسی، قطار یا هواپیما را ترک می‌کنید، یک بررسی سریع از دستگاههای خود انجام داده و مطمئن شوید که همه دستگاههای خود را به همراه دارید. فراموش نکنید که به دوستان و اعضای خانواده نیز که همراه شما سفر میکنند یادآوری کنید که دستگاههای خودشان را مجددا بررسی کنند، مانند کودکانی که ممکن است دستگاهی را روی یک صندلی یا داخل رستوران جا بگذارند.

  در مورد دستگاه‌هایی که انتخاب می‌کنید تا همراهتان بیاورید، مطمئن شوید که آنها را به‌روزرسانی کرده‌اید تا از آخرین نسخه ی سیستم عامل و برنامه‌ها استفاده کنند. قفل صفحه را فعال نگه دارید. در صورت امکان، مطمئن شوید که راهی برای ردیابی از راه دور دستگاه های خود در صورت گم شدن آنها دارید. علاوه بر این، ممکن است بخواهید گزینه ای برای پاک کردن از راه دور دستگاهتان داشته باشید. به این ترتیب، اگر دستگاهی گم یا دزدیده شود، می توانید از راه دور همه داده های حساس و حساب های خود را ردیابی و (یا) از دستگاه حذف کنید. در نهایت، از هر دستگاهی که همراه خود میبرید یک نسخه پشتیبان تهیه کنید تا در صورت گم شدن یا دزدیده شدن یکی از آنها، به راحتی بتوانید اطلاعات خود را بازیابی کنید.

- اتصال به شبکه های بی سیم: در هنگام سفر، ممکن است لازم باشد به یک شبکه Wi-Fi عمومی متصل شوید. به خاطر داشته باشید که اغلب نمی دانید چه کسی آن شبکه Wi-Fi را پیکربندی کرده است، چه کسی یا چگونه آن را نظارت می کند، و چه شخص دیگری به آن متصل است. در صورت امکان به جای اتصال به یک شبکه Wi-Fi عمومی، به هات-اسپات شخصی تلفن هوشمند خود متصل شوید و از آن استفاده کنید. به این ترتیب می دانید که یک اتصال Wi-Fi قابل اعتماد دارید. اگر این امکان برای شما وجود ندارد و باید به یک شبکه Wi-Fi عمومی (مانند داخل فرودگاه، هتل یا کافه) متصل شوید، از یک شبکه خصوصی مجازی که اغلب VPN نامیده می شود استفاده کنید. این نرم‌افزاری است که روی لپ‌تاپ یا دستگاه‌های تلفن همراه خود نصب می‌کنید تا به محافظت و ناشناس کردن اتصال Wi-Fi شما کمک کند. برخی از راه حل های VPN شامل تنظیماتی برای فعال کردن خودکار VPN هنگام اتصال به شبکه های Wi-Fi غیر قابل اعتماد هستند.

- **رایانه های همگانی**: از استفاده از رایانه های عمومی و همگانی، مانند رایانه های موجود در لابی هتل ها یا کافی شاپ ها، برای ورود به هر یک از حسابهای کاربری یا دسترسی به اطلاعات حساس اجتناب کنید. شما نمی دانید چه کسی قبل از شما از آن رایانه استفاده کرده است، و ممکن است آن را به طور تصادفی یا از روی عمد با بدافزار آلوده کرده باشد، مانند بدافزار ثبت کننده صفحه کلید(keystroke logger). از دستگاه هایی که به آنها اعتماد دارید و توسط شما کنترل میشوند استفاده کنید.

- رسانه های اجتماعی: ما عاشق این هستیم که دیگران را در مورد سفرها و ماجراهای خودمان از طریق رسانه های اجتماعی به روز و با خبر کنیم، اما همیشه نمی دانیم که کدام دوست یا بیننده ای آنلاین است. تا حد ممکن در تعطیلات از اشتراک گذاری بیش از حد خودداری کنید و برای به اشتراک گذاشتن سفر خود تا رسیدن به خانه منتظر بمانید. علاوه بر این، تصاویر کارت پرواز، گواهینامه رانندگی، یا گذرنامه را ارسال نکنید و به اشتراک نگذارید، زیرا ممکن است منجر به سرقت هویت شود.

- کار: اگر قرار است در تعطیلات کار کنید (امیدواریم که جوابتان منفی باشد!)، مطمئن شوید که سیاست‌های سفر کاری خود را زودتر از موعد بررسی کرده‌اید، مانند اینکه چه دستگاه‌ها یا داده‌هایی را می‌توانید همراه خود بیاورید و چگونه از راه دور میتوانید به سیستم‌های کاری تان به صورت امن متصل می شوید.

تعطیلات باید زمانی برای استراحت، سیاحت و تفریح باشد. این مراحل ساده به شما کمک می کند تا مطمئن شوید که این کار را با خیال راحت و به صورت امن انجام می دهید.

سردبیر مهمان

پرنسس یانگ یک تحلیلگر ارشد در خطوط هوایی Southwest است و تلاشهای آموزشی و پرورشی امنیت سایبری را برای 60,000 کارمند در سراسر کشور رهبری می کند. پرنسس به گونه ای با کارمندان خود رفتار میکند تا آنها بتوانند با احساس شوق و انرژی فراوان بدون در نظر گرفتن نقش یا عنوان خود، مسئولیت امنیت سایبری را به اشتراک بگذارند.

منابع

اااستفاده ایمن از دستگاههای تلفن همراه: https://www.sans.org/newsletters/ouch/securing-mobile-devices/

قدرت به روز رسانی: https://www.sans.org/newsletters/ouch/the-power-of-updating/

شبکه های خصوصی مجازی: https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/

پشتیبان گیری دارم: https://www.sans.org/security-awareness-training/resources/got-backups

ترجمه شده برای عموم توسط: سعید میرجلیلی، مجید هدایتی