

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

میخواهید به مسافرت بروید؟ چند گام ساده برای ایجاد امنیت سایبری

مقدمه

فصل تابستان در راه است و به زودی میلیون ها نفر به سراسر جهان سفر خواهند کرد. اگر به تعطیلات می روید، در اینجا چند نکته در مورد سفرتان وجود دارد که به شما کمک می کند تا در فضای مجازی هوشیار و ایمن باشید.

دستگاه های موبایل

از بسته بندی و حمل بیش از حد خودداری کنید: فقط هنگام رفتن به تعطیلات، دستگاه های تلفن همراه مورد نیاز و ضروری خود را همراه داشته باشید. منظور ما از دستگاه های تلفن همراه، دستگاه هایی از جمله لپ تاپ، تبلت، گوشی های هوشمند، ساعت های هوشمند، کتابخوان های الکترونیکی و دستگاه های بازی قابل حمل است. هر چه دستگاه های کمتری در سفر به همراه داشته باشید، دستگاه های کمتری ممکن است گم شده یا دزدیده شوند. در واقع، آیا می دانستید که احتمال گم شدن یک دستگاه تلفن همراه بسیار بیشتر از دزدیده شدن آن است؟ اغلب اوقات فقط پیگیری دستگاه های خود می تواند بزرگترین چالش شما باشد. این عادت را در خودتان ایجاد کنید که هرگاه اتاق هتل، رستوران، تاکسی، قطار یا هواپیما را ترک می کنید، سریع دستگاه خود را بررسی کرده و مطمئن شوید که همه دستگاه های خود را به همراه دارید. فراموش نکنید که دوستان یا خانواده با شما در سفر باشند تا دستگاه های شما را هم چک کنند - به ویژه کودکانی که ممکن است دستگاهی را روی صندلی یا رستوران بگذارند.

در مورد دستگاه هایی که همراه خودتان می آورید، مطمئن شوید که سیستم عامل و برنامه ها را قبل خروج از منزل به روزرسانی کرده اید تا آخرین نسخه ها را اجرا کنند. اغلب اوقات ساده ترین راه برای انجام این کار، فعال کردن به روزرسانی خودکار در دستگاه است. این کار تضمین می کند که دستگاه های شما هر گونه آسیب پذیری وصله شده دارند و آخرین ویژگی های امنیتی را اجرا می کنند. قفل صفحه را فعال نگه دارید، و 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 پاک کردن از راه دور دستگاه را از قبل فعال کنید. 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 با خود می برید یک نسخه پشتیبان تهیه کنید تا در صورت گم شدن یا دزدیده شدن یکی از آنها، بتوانید به راحتی اطلاعات خود را بازیابی کنید.

اتصالات شبکه بی سیم (Wi-Fi)

هنگام سفر، ممکن است بخواهید به یک شبکه Wi-Fi عمومی متصل شوید. نمونه هایی از شبکه های Wi-Fi عمومی شامل شبکه های Wi-Fi رایگان در فرودگاه، کافی شاپ یا رستوران ها است. به خاطر داشته باشید، شما اغلب نمی دانید که چه کسی یک شبکه Wi-Fi معین را پیکربندی کرده است، چه کسی آن را نظارت می کند یا چگونه، و چه فرد دیگری به آن متصل است. به جای اتصال به یک شبکه Wi-Fi عمومی، در صورت امکان، از ویژگی hotspot شخصی تلفن هوشمند خود برای اتصال دستگاه های شخصی خود به اینترنت استفاده کنید. به این ترتیب می دانید که یک اتصال Wi-Fi قابل اعتماد دارید.

نکته دیگر برای کاهش حجم داده ای که در تعطیلات خود استفاده می کنید این است که قبل از عزیمت به سفر، آنچه را که در خانه نیاز دارید دانلود کنید. این می تواند شامل دانلود نسخه های نقشه ها برای پیمایش آسان مقصد به صورت آفلاین در برنامه ناوبری دلخواه یا دانلود هر گونه سرگرمی دیجیتالی از قبل مانند کتاب های صوتی، کتاب های الکترونیکی، بازی ها یا فیلم ها باشد.

کامپیوترهای عمومی

هرگز از رایانه های عمومی مانند رایانه های موجود در لابی هتل ها یا کافی شاپ ها برای ورود به هر حساب یا دسترسی به اطلاعات حساس استفاده نکنید. شما نمی دانید چه کسی قبل از شما از آن رایانه استفاده کرده است، و ممکن است آنها به طور تصادفی یا عمدتاً آن رایانه را با بدافزار آلوده کرده باشند، مانند ثبت کننده ضربه زدن به کلید (keystroke logger). به دستگاه های خود که کنترل و اعتماد دارید بچسبید.

رسانه های اجتماعی

همه ما دوست داریم دیگران را در مورد ماجراهای خود از طریق رسانه های اجتماعی به روز کنیم، اما شما نمی دانید چه کسی همه پست های شما را خواهد خواند. تا حد امکان از اشتراک گذاری بیش از حد در تعطیلات خودداری کنید و منتظر بمانید تا ماجراجویی های خود را تا زمانی که از سفر خود به خانه برگردید به اشتراک بگذارید. همچنین، تصاویر کارت پرواز، گواهینامه رانندگی یا گذرنامه را پست نکنید، زیرا ممکن است منجر به سرقت هویت شود.

آداب و رسوم و قوانین محلی

قوانین کشوری که از آن بازدید می کنید را بررسی کنید. حقوق قانونی شما از یک کشور به کشوری دیگر متفاوت است. محتوایی که ممکن است در خانه قابل تحمل باشد ممکن است در کشور دیگری غیرقانونی باشد. مواردی که باید قبل از رفتن بدانید

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

ماريسا میدلر یک مهندس امنیت سایبری در بخش CERT در موسسه مهندسی نرم افزار دانشگاه کارنگی ملون است. ماریسا یک متخصص امنیت سیستم های اطلاعاتی (CISSP) است و دارای مدرک در دانشگاه کارنگی ملون (MS) و دانشگاه پیتسبورگ (BS/BA) است.

منابع

قدرت به روز رسانی: <https://www.sans.org/newsletters/ouch/the-power-of-updating>
محركهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: <https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you>
یک قدم ساده برای امن کردن حسابهای شما: <https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts>

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو

IOUCH توسط SANS Security Awareness منتشر شده است و تحت مجوز Creative Commons BY-NC-ND 4.0 می باشد. شما آزاد هستید که این ماهنامه را برای بقیه اشتراک گذاشته یا آن را توزیع نمایید به شرطی که آن را به فروش نرسانده یا تغییری در آن ایجاد نکنید. هیئت تحریریه: Princess Young, Leslie Ridout, Alan Waggoner, Phil Hoffman, Walter Scrivens.