ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- قبل از سفر
- دستگاه های گم کرده / به سرقت رفته
- دسترسی به Wi-Fi
- کامپیوترهای عمومی

سفری امن

مقدمه

در این شماره در مورد اینکه چگونه وقتی در مسافرت هستید میتوانید بصورت امن به اینترنت وصل شوید و کارهایتان را انجام دهید، بحث میکنیم.

سردبیر مهمان

سردبیر مهمان: استیو آرمسترانگ (Steve Armstrong) مدیر فنی CyberCPR در شرکت Logically Secure همچنین مربی مورد تایید SANS و نویسنده سابق کتابهای درسی موسسه SANS است. او در توییتر با شناسه **@Nebulator** و در گوگل پلاس با شناسه **+SteveArmstrongSecurity** فعال است.

قبل از سفر

در حالی که شبکه شما در خانه یا شبکه محل کارتان ممکن است امن باشد، ولی زمانی که در سفر هستید، همیشه باید فرض کنید که هر شبکه ای که وصل میشوید غیر قابل اعتماد است. هرگز نمی دانید که چه کسان دیگری بر روی آن شبکه هستند و چه خطرهایی از جانب انها یا آن شبکه برای شما در برخواهد داشت. برخی از اقدامات ساده قبل از سفر می تواند کمک بزرگی به حفاظت از اطلاعات شما در طی سفر بکند. یک یا دو هفته قبل از سفر خود:

- داده هایی که نیازی به همراه داشتن آن ندارید و بر روی دستگاهتان است را شناسایی کنید و هر گونه اطلاعات غیر ضروری را حذف کنید. این به طور قابل توجهی می تواند در کاهش تبعات منفی که ممکن است در اثر گم کردن، دزدیده شدن یا از دست دادن یا توقیف توسط گمرک یا کارکنان امنیت مرزی شما را تهدید کند، کمک کند. اگر سفری کاری است از سرپرست خود بپرسید که آیا سازمان شما دستگاهی جایگزین که به طور خاص برای کار در حال سفردر نظر گرفته شده است دارد تا استفاده کنید.
- برای مسافرت های بین المللی، بررسی کنید چه نوع پریز برق در آن کشور استفاده می شود، چون ممکن است نیاز به آداپتوری برای شارژ دستگاهتان داشته باشید. علاوه بر این، بررسی کنید که چه قراردادی با شرکت مخابراتی ارائه دهنده خدمات تلفن همراه دارید، شرکتها اغلب هزینه بالایی برای استفاده از داده در سفرهای خارجی میگیرند، ممکن است بخواهید قابلیت های داده تلفن همراه خود را در حالی که در سفر خارجی هستید را غیر فعال کنید و یا قرارداد خدمات خود را برای مسافرت های بین المللی تغییر دهید.
- نرم افزار ردیابی بر روی دستگاه خود نصب کنید، تا بتوانید از راه دور ردیابی کنید که دستگاه شما کجاست، و حتی اگر آن را از دست دادید و یا به سرقت رفت از راه دور اطلاعات آن را پاک کنید. بسیاری از دستگاه های تلفن همراه در حال حاضر این قابلیت را در خود دارند و فقط ممکن است باید آن را فعال کنید (به یاد داشته باشید که این امکان نیاز به دسترسی به اینترنت دارد تا کار کند)

یک یا دو روز قبل از سفر:

- دستگاه ها، برنامه ها و نرم افزار ضد ویروس را به روز رسانی کنید تا حتما آخرین نسخه را داشته باشید.
- تمام تنظیمات امنیتی مناسب مانند فایروال را بر روی دستگاه خود فعال کنید.
- بر روی تمام دستگاه های قابل حمل مثل تلفن همراه خود رمز عبوری قوی و یا کد عبور بگذارید. به این ترتیب اگر دستگاه خود را

سـفری امن

از دست دادید و یا به سرقت رفت، دیگران نمی توانند به اطلاعات شما بر روی آن دسترسی پیدا کنند.

- تمام اطلاعات روی دستگاه های خود را رمزگذاری کنید به طوری که اگر آنها را از دست دادید و یا به سرقت رفت، داده ها قابل استفاده برای کسی نباشد. برخی دستگاه ها مانند اپل این کار را به طور خودکار انجام میدهند اگر شما رمز عبور یا کد عبوری بر روی دستگاه بگذارید.
- پشتیبان کامل از تمام دستگاه های خود تهیه کنید. به این ترتیب اگر در حین سفر اتفاق برای دستگاهها یا داده های روی آنها افتاد، باز نسخه دیگری از داده ها را در جای امنی دارید.

نکته کلیدی در امن ماندن در حالی که در سفرهستید، امن کردن دستگاه های خود قبل از خروج از خانه، امن نگه داشتن فیزیکی آنها و دانستن اینکه در هر لحظه کجا هستند، و رمزگذاری تمام فعالیت های آنلاین میباشد.

دستگاههای از دست داده / سرقت شده

هنگامی که سفر خود را شروع میکنید در مورد ایمنی فیزیکی دستگاه های خود مطمئن شوید. به عنوان مثال، هرگز دستگاه خود را در ماشین که مردم میتوانند به راحتی داخل آن را ببینند جا نگذارید، چون تبهکاران به سادگی پنجره ماشین را شکسته و بدون سر و صدا و با شتاب هر چیزی ارزشداری که بتوانند را بسرقت میبرند. یک راه حل این است که کابل و قفل با خود همراه داشته باشید تا از لحاظ فیزیکی بتوانید دستگاهای خود مانند لپ تاپ را هنگامی که آنها را ترک میکنید قفل کنید. در حالی که خطر دزدیدن هست، چیزی که ممکن است مطلع نباشید این است که احتمال گم کردن یا جاگذاشتن دستگاه بیشتر از به سرقت رفتن آن است. با توجه به مطالعه انجام شده توسط ورایزون در بازه ده ساله، احتمال از دست دادن یک دستگاه۵۱ برابر بیشتر از سرقت رفتن آن است. این به این معنی است که همیشه دقت کنید که دستگاه های خود را در هنگام سفر همراه داشته باشید، مثلا زمانی که وسائلتان را بعد از کنترل امنیتی در فرودگاه بر میدارید، یا تاکسی یا رستوران را ترک میکنید، یا هتل را ترک میکنید و یا قبل از ترک هواپیما.

دسترسی Wi-Fi

دسترسی به اینترنت در سفر اغلب با استفاده از نقاط دسترسی Wi-Fi عمومی است، مانند اینترنت بی سیمی که درداخل هتل، کافی شاپ و یا در فرودگاه هست. مشکل اینترنت Wi-Fi عمومی این است نه تنها شما هرگز نمیدانید که چه کسی آنها را راه اندازی کرده، بلکه هیچ وقت نمی دانید که چه کسانی به آنها متصل هستند. به این دلیل آنها غیر قابل اعتماد در نظر گرفته میشوند، در واقع به این دلیل شما باید تمام اقدامات را برای امن کردن دستگاه های خود قبل از ترک آنها انجام دهید. علاوه بر این، فن آوری Wi-Fi از امواج رادیویی برای برقراری ارتباط از دستگاه شما به نقطه دسترسی بی سیم استفاده میکند. این به این معنی است که هر کسی بطور فیزیکی در نزدیکی شما باشد به طور بالقوه می تواند بر ارتباطات شما رهگیری و نظارت داشته باشد.

به همین دلیل است که اگرز Wi-Fiعمومی استفاده میکنید، حتما فعالیت های آنلاین شما رمزگذاری شده باشد. به عنوان مثال، هنگام اتصال آنلاین با استفاده از مرورگر خود مطمئن شوید وب سایت هایی که بازدید میکنید رمزگذاری شده هستند (یعنی در آدرس وبسایت نوشته شده

سـفری امن

باشـد https:// و یـک تصویـر قفـل بسـته هـم بـالای صفحـه باشـد) عـلاوه بـر ایـن، ممکـن اسـت شـما از VPN (شـبکه خصـوصی مجـازی) اسـتفاده کنیـد کـه همـه فعالیـت هـای آنلایـن شـما رمزگـذاری خواهـد بـود. ایـن امـکان VPN ممکـن اسـت بـه شـما از طریـق محـل کار داده شـود، و یـا شـما مـی توانیـد بـرای اسـتفاده شـخصی خـود خریـده باشـید. اگـر شـما نگـران آن هسـتند کـه هیـچ نقطـه دسـترسی Wi-Fi کـه بتوانیـد اعتمـاد کنیـد وجـود نـدارد، میتوانیـد بـه گـوشی هـای هوشـمند متصـل شـوید و از اینترنـت آن اسـتفاه کنیـد. (هشـدار: همانطـور کـه پیشـتر اشـاره شـد، ایـن مـی توانـد گـران قیمـت باشـد وقـتی در مسـافرت بـین المللی هسـتید، اول بـا ارائـه دهنـده خدمـات تلفـن همـراه خـود صحبـت کنیـد)

منابع عمومی

از کامپیوترهـای عمومـی، ماننـد کامپیوتـر در لابی هتـل، کتابخانـه و یـا در کافـه هـای اینترنـتی اسـتفاده نکنیـد. شـما هیـچ نمیدانیـد کـه قبـل از شـما چـه کـسی از آن کامپیوتـر اسـتفاده کـرده اسـت، آنهـا ممکـن اسـت آن کامپیوتـر عمومـی را بـه طـور تصـادفی یـا بـه عمـد آلـوده کـرده باشـند. در صـورت امـکان، تنهـا از دسـتگاه هـایی کـه کنـترل روی آنهـا داریـد و بـه آنهـا اعتمـاد داریـد بـرای هـر گونـه فعالیـت آنلایـن اسـتفاده کنیـد. اگرمجبوریـد رایانـه ای عمومـی اسـتفاده کنیـد، از هیـچ سرویـسی کـه نیـاز بـه ورود رمـز عبـور بـرای ورود بـه سیسـتم دارد اسـتفاده نکنیـد.

بیشتر بدانید

بـا مراجعـه بـه آدرس زیـر، مشـترک ماهنامـه OUCH! شـوید و بـه آرشـیو خبرنامـه آگاهـی از امنیـت OUCH! دسـترسی داشـته باشـید، و در مـورد راه حل‌هـای افزایـش آگاهی‌هـای امنیـتی موسسـهSANS بیشـتر بدانیـد.

آدرس: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

رمز عبور:	http://www.securingthehuman.org/ouch/2013#may2013
تأیید دو مرحله ای:	http://www.securingthehuman.org/ouch/2013#august2013
رمزگذاری:	http://www.securingthehuman.org/ouch/2014#august2014
امن کردن تبلت جدیدتان:	http://www.securingthehuman.org/ouch/2013#december2013
مطالعه ورایزون سال 2004:	http://www.verizonenterprise.com/DBIR/2014/

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus