ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- بررسی قبل سفر
- وسایل گم شده یا دزدیده شده
- دسترسی به شبکه های بی سیم
- کامپیوترهای همگانی

سفری امن داشته باشید

مقدمه

هدف ما این است که به شما کمک کنیم تا بتوانید حداکثر استفاده را از تکنولوژی - حتی در مسافرت - ببرید. در این خبرنامه به شما خواهیم گفت که چگونه ابزار خود را در طول مسافرت بصورت امن به اینترنت وصل کنید و از آن استفاده کنید.

سردبیر مهمان

مارک ویلیام، معمار امنیت در شرکتها است که برای بلوکراس بلوشیلد در ایالت تنسی کار میکند. وی همچنین بعنوان مدرس SANS و رییس ISSA(Information Systems Security Association) در حوزه چاتانگا (شهری در جنوب غربی ایالت تنسی) میباشد. مارک بدلیل مسافرتهای فراوان، شناخت خوبی دارد نسبت به مسائل امنیتی که ممکن است اتفاق بیافتد برای دستگاههایی که در مسافرت همراه دارید.

بررسی قبل از سفر

با فرض اینکه شبکه شما در خانه و یا محل کار ممکن است امن باشد باید توجه داشته باشید شبکه هایی که در طول مسافرت به آن وصل میشوید به هیچ عنوان قابل اعتماد نیستند. شاید شما ندانید که آیا شخص دیگری در آن شبکه است و یا در حال انجام چه کاری است.قدم های ساده ای که لازم است قبل از مسافرت و به منظور حفاظت از خود و داده های خود بردارید به شرح ذیل است :

- اطلاعات زمانی امن تر هستند که شما آنها را بهمراه نداشته باشید .برای این منظور بهتر است داده هایی را که نیاز نیست بهمراه تجهیزات خود داشته باشید را شناسایی و سپس آنها را حذف کنید.با این کار میتوانید تا حد قابل توجهی اثرات مخرب ناشی از گم کردن تجهیزات ، دزدی و یا توقیف آنها در گمرکات و یا مرزهای امنیتی بکاهید. درصورتیکه به مسافرت کاری میروید از سرپرست خود بپرسید که آیا شرکت برای مسافرت های کاری تجهیزات مختص مسافرت ارائه میدهد یا خیر.
- موبایل و لب تاپ خود را با استفاده از پسوردهای سخت قفل کنید. بدین ترتیب در صورت دزدیده و یا گم شدن تجهیزات ،امکان دسترسی به اطلاعات موجود در آنها وجود نخواهد داشت. علاوه بر این رمزگذاری کامل حافظه را بر روی موبایل و یا لب تاپ خود فعال نمایید. در بسیاری از تجهیزات موبایلی وقتی قفل دسترسی روی دستگاه میگذارید، رمزگذاری بصورت خودکار فعال میشود.
- نرم افزاری بر روی دستگاه نصب کنید که در صورت گم شدن و یا دزدیده شدن آن بتوانید از راه دور آن را ردیابی کنید و یا حتی اطلاعات آن را از راه دور پاک کنید.
- قبل از سفر، دستگاه ها ، برنامه ها و آنتی ویروس خود را بروز کنید و مطمئن شوید که آخرین ویرایش در حال اجراست. بسیاری از حملات بر روی دستگاه هایی رخ میدهند که نرم افزار های بروز ندارند.
- از کلیه دستگاه های خود پشتیبان بگیرید. بدین ترتیب اگر در طول مسافرت اتفاق برای آن بیافتد شما همچنان اطلاعات اصلی خود را در جای امن نگه داشته اید .

سفری امن داشته باشید

- قبل از مسافرت خارجی میبایست بررسی کنید که چه طرح خدماتی از طرف شرکت ارائه دهنده خدمات موبایلی بر روی گوشی شما فعال است. اغلب سرویس دهندگان موبایل برای استفاده از داده فرامرزی هزینه بالاتری را مطالبه میکنند لذا شما ممکن است بخواهید در زمان مسافرتهای برون مرزی خدمات داده را برای تلفن خود غیر فعال نمایید و یا سیم کارت محلی پیش پرداخت شده تهیه نمایید.

برای امن ماندن در طول مسافرت، دستگاههایتان را قبل سفر امن کنید، مواظب باشید گم نکنید یا دزدیده نشوند و همه داده های بر خط را رمزگذاری کنید.

گم شدن / دزدیده شدن دستگاه ها

به محض اینکه مسافرت خود را شروع کردید از امنیت فیزیکی دستگاه های خود اطمینان حاصل کنید.بعنوان مثال ، به هیچ عنوان تجهیزات خود را در داخل ماشین که به راحتی قابل دیدن است نگذارید در این صورت ممکن است افراد بزهکار پس از شکستن شیشه خودرو هر چیز با ارزشی که میبینند را بدزدند. گرچه دزدیدن وسایل شما محتمل است ولی بر اساس تحقیقات اخیر Verizon ، احتمال اینکه مردم وسایل خود را گم کنند صد برابر بیشتر از دزدیده شدن آن است. بنابراین همیشه در طول مسافرت با بررسی مجدد مطمئن شوید که وسایل خود را فراموش نکرده اید .بعنوان مثال زمانیکه در فرودگاه در حال عبور از بخش امنیتی هستید و یا در حال پیاده شدن از تاکسی و یا خروج از رستوران هستید و یا در حال تحویل اتاق هتل خود هستید و یا قبل از پیاده شدن از هواپیما هستید بررسی کنید که وسایل خود را فراموش نکرده اید.

دسترسی به شبکه های بیسیم

دسترسی به اینترنت در طول مسافرت به معنی استفاده از اکسس پوینت های عمومی نظیر هتل ، کافی شاپ و یا فرودگاه است. استفاده از این شبکه های بیسیم عمومی دارای دو اشکال اساسی است .اولا شما نمیدانید که چه کسی آنها را راه اندازی کرده و ثانیا چه کسانی به آنها وصل هستند. به این دلیل میبایست آنها را نامطمئن دانست و حقیقت این مسئله که چرا باید قبل از مسافرت تجهیزات خود را امن کنید همین است. علاوه بر این، در شبکه بی سیم از امواج رادیویی استفاده میشود و این به این مفهوم است که افرادی در نزدیکی شما بطور بالقوه قابلیت ترجمه و نظارت بر ارتباطات شما را دارند. به همین دلیل در صورتیکه از شبکه های بی سیم عمومی استفاده میکنید، میبایست حتما کلیه فعالیت های برخط شما رمزگذاری شود. بعنوان مثال زمانیکه با مرورگر خود و بصورت برخط به سایتی وصل میشوید مطمئن شوید که ارتباط شما رمزگزاری شده است.در این صورت میتوانید با پیدا کردن کلمه «HTTPS://» و یا شکل یک قفل بسته را کنار آدرس URL خود از رمزگذاری شدن آن ارتباط مطمئن شوید.علاوه بر این شما ممکن است از VPN(Virtual Private Network) استفاده کنید که قادر است کلیه فعالیت های برخط شما را رمزگذاری کند. VPN ممکن است از طرف شرکت برای شما فعال شود و یا ممکن است شما برای استفاده شخصی آن را خریداری کنید. اگر نگران هستید که نتوانید شبکه بی سیم مطمئنی را بیابید میتوانید از اینترنت

سفری امن داشته باشید

گوشی هوشمند خود استقاده کنید. هشدار: همانگونه که قبلا گفته شد استفاده از اینترنت همراه در مسافرت های فرامرزی میتواند گران باشد . لازم است هزینه ها را با شرکت ارائه دهنده خدمات بررسی کنید.

کامپیوترهای همگانی

هرکز از کامپیوتر های همگانی نظیر کامپیوتر های موجود در لابی هتل ها و یا کافی نت ها برای ورود به حساب ها و دسترسی به اطلاعات حساس استفاده نکنید. شما نمی دانید چه کسانی قبلا از آن کامپیوتر ها استفاده کردند و ممکن است عمدی و یا سهوی آنها را آلوده کرده باشند. در صورت امکان تنها از دستگاههایی استفاده کنید که مطمئن و قابل کنترل هستند. در بهترین حالت، کامپیوتر های عمومی تجهیزاتی مناسب برای دریافت اطلاع از وضعیت آب و هوا و یا خواندن اخبار هستند. ورود به هر نوع حساب شخصی نظیر حساب گوگل میتواند چراغ سبزی برای هکرها باشد که ممکن است شما را تحت نظر گرفته باشند .

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در:

www.safenet-co.net

منابع

گذرعبارت:	https://securingthehuman.sans.org/ouch/2015#april2015
پشتبان گیری:	https://securingthehuman.sans.org/ouch/2015#august2015
بدافزار:	https://securingthehuman.sans.org/ouch/2016#march2016
رمزگذاری:	https://securingthehuman.sans.org/ouch/2016#june2016
آرشیو ترجمه های خبرنامه وای!:	https://securingthehuman.sans.org/ouch/archives

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی