

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

خانه رومی دیجیتال

مقدمه

بسیاری از ما منتظر بهار هستیم مناظر زیبا در حال شکل گیری است، گل ها شروع به شکوفه می کنند و بسیاری از ما بهار زمان خانه رومی است. در حالی که خانه رومی، تمیز و مرتب کردن معمول به نظر می آید، اما لزوم نیاز به همچنین خانه رومی دیجیتال ممکن است چندان آشکار نباشد. در اینجا چند نکته کوتاه برای منظم کردن زندگی دیجیتالی و ایجاد عادات جدید دیجیتال آورده شده است:

پشتیبان گیری: ما این مورد را اول ذکر میکنیم زیرا در طولانی مدت، این یکی از مهمترین و البته گامی است که قبل از کارهای دیگر باید انجام دهید. مهم نیست که چقدر موارد ایمنی را رعایت میکنید، بعضی وقتها، شما به احتمال زیاد به بازیابی اطلاعات مهم خود نیاز دارید که اهمیت پشتیبان گیری مشخص خواهد شد. دلایل استفاده از پشتیبان می تواند شامل خرابی هارد دیسک، از دست دادن دستگاهی یا آلوده شدن به بد افزارهایی مانند باج افزارها باشد. ایجاد و برنامه ریزی پشتیبان گیری خودکار به شما اطمینان می دهد که می توانید مهمترین اطلاعات خود را در زمان نیاز بازیابی کنید.



حذف: برنامه ها یا برنامه های بلااستفاده در دستگاه های تلفن همراه و رایانه های خود را حذف کنید. برخی از برنامه ها به مقادیر زیادی فضای ذخیره سازی نیاز دارند، که می توانند آسیب پذیری های جدیدی را برای شما ایجاد کنند و حتی ممکن است سرعت آن را کند کنند. هرچه برنامه های کمتری داشته باشید، سیستم و اطلاعات شما از امنیت بیشتری برخوردار است. بسیاری از دستگاه ها به شما آخرین باری که از برنامه ای استفاده کرده اید را نشان میدهند. اگر بیش از چند ماه بیشتر باشد، احتمال دارد که به برنامه نیاز نداشته باشید!



به روز رسانی: همه دستگاه ها و برنامه های خود را به روز کنید و هر جا ممکن است به روز رسانی خودکار را فعال کنید. به این ترتیب، دستگاه ها و برنامه های شما به روز میمانند، نه تنها عملکرد آنها سریع تر خواهد بود، بلکه هک کردن آنها نیز بسیار سخت تر خواهد بود.



گذر واژه ها: آنها را بازنگری کنید. اگر از چندین رمز عبور یکسان برای چندین حساب استفاده می کنید، آنها را تغییر دهید تا هر حساب دارای یک رمز عبور منحصر به فرد باشد. نمی توانید تمام رمزهای عبور منحصر به فرد خود را به خاطر بسپارید؟ از نرم افزارهای مدیریت گذرواژه استفاده کنید. همچنین از تأیید اعتبار دو عاملی (2FA) هر جا ممکن است استفاده کنید، خصوصاً برای هرگونه ایمیل یا حساب کاربری مالی (مانند حساب بانک اینترنتی) فعال کنید.





حساب های مالی: حتما حساب های بانکی، حساب های کارت اعتباری و حساب های بازنشستگی به گونه ای تنظیم شوند که هر زمان تراکنشی انجام شد، به خصوص برای خریدهای بزرگ یا نقل و انتقال پول زیاد، به شما هشدار دهند. هرچه زودتر متوجه فعالیت های کلاهبردارانه شوید، زودتر می توانید جلوی آن را بگیرید. بسته به اینکه در کدام کشور زندگی می کنید، بستن حساب اعتباری می تواند یکی از موثرترین راههای محافظت از هویت شما باشد.



مرورگر: همه افزونه ها و یا پلاگین های نصب شده در مرورگر خود را بازنگری کنید. تنظیمات مجوز داده شده به افزونه ها را مرور کنید. آیا این افزونه ها واقعا نیاز به دسترسی به موقعیت مکانی، رمز عبور یا لیست تماس های شما دارند؟ اگر دیگر از افزونه های خاصی استفاده نمی کنید، یا نگرانی هایی درباره میزان رعایت حریم خصوصی توسط آنها دارید، آنها را حذف کنید.



شبکه های اجتماعی: حضور آنلاین خود را بررسی کنید. تنظیمات حریم خصوصی خود را مرور کنید و هرگونه عکس و فیلم که دیگر به آنها دسترسی ندارید یا نیاز ندارید، حذف کنید. همچنین می توانید خود را در موتورهای جستجو جستجو کنید و ببینید چه اطلاعاتی در مورد شما وجود دارد. به یاد داشته باشید، خوب است که میزان اطلاعاتی را که به اشتراک می گذارید را محدود کنید، و حتی اینکه با چه کسی تصمیم دارید آن را به اشتراک بگذارید.



میز کار: کشو میز کار خود را تمیز کنید، هر دیسک درایو قدیمی یا فلش USB که اطلاعات غیر نیاز روی آن است را پاک کنید. حتی یادداشت ها با اطلاعات بیش از حد نیاز را از بین ببرید. در صورتی که دستگاه خردکننده اسناد ندارید، بد نیست که بخرید.



ایمیل: ایمیل ها و فایل های ضمیمه آنها که لازم ندارید را حذف کنید و آنچه نگه میدارید را سازماندهی کنید. به مدارک حساس مانند آنهایی که تاریخ تولد یا شماره تأمین اجتماعی خود را دارند توجه ویژه داشته باشید و آن را از پوشه ایمیل های وارده خود خارج کنید!

اگرچه به نظر این پاکسازی ها یک کار وقت گیر به نظر می آید، اما مطمئن باشید که دستگاه ها و اطلاعات شما محفوظ خواهند ماند و درد سرهای بعدی کمتری خواهید داشت. اگر همه این کارها که گفتیم زیاد به نظر می آید، فقط چند مورد را انتخاب کنید یا سعی کنید یک مورد را در روز یا هفته انجام دهید. هر قدم کوچکی بردارید، قدم بزرگی در راه محافظت از شما خواهد بود.



سر دبیر مهمان

کتی نیکلز [@LiketheCoins](#) یک تحلیلگر ارشد اطلاعات شرکت Red Canary و همچنین مربی موسسه SANS در درس FOR578: Cyber Threat Intelligence است. وی بیش از یک دهه در زمینه امنیت شبکه، واکنش سریع و بخش اطلاعات تهدید سایبری فعالیت داشته است.

منابع

پشتیبان بگیرید:

آسان سازی گنرواژه ها

خود را جستجو کنید:

نکاتی لازم قبل از فروش یا دور انداختن وسایل الکترونیکی موبایل:

<http://www.sans.org/u/Z2Q>

<http://www.sans.org/u/Y63>

<http://www.sans.org/u/ZVB>

<http://www.sans.org/u/ZVG>

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND 4.0 منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفا با www.sans.org/security-awareness/ouch-newsletter تماس بگیرید. هیأت تحریریه: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | ترجمه شده توسط: سعید میرجلیلی، مجید هدایتی