ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

رسانه های اجتماعی

مقدمه

سایت های رسانه های اجتماعی مانند فیس بوک، توییتر، اینستاگرم و LinkedIn سایتهای شگفت انگیزی هستند که به شما امکان ملاقات، تعامل و به اشتراک گذاری اطلاعات با مردم سراسر جهان را میدهند. با این حال، همراه با تمام این امکانات خطراتی هم هست، نه فقط برای شما، بلکه برای خانواده، دوستان و کارفرمای شما. در این خبرنامه توضیح میدهیم چه خطراتی وجود دارد و چگونه از این سایتها ایمن و بدون خطر استفاده کنیم.

سردبیر مهمان

تانیا باکام (Tanya Baccam) یک مشاور امنیتی باسابقه است. برای بیش از یک دهه، او نویسنده کتب و مربی موسسه SANS بوده است، از جمله AUD507، MGT414، SEC401، SEC542، SEC502 و بسیاری از دوره های دیگر. او را در توییتر با نشانی **@tbaccam** دنبال کنید.

حفظ حریم خصوصی

یک نگرانی مشترک در مورد رسانه های اجتماعی حفظ اطلاعات شخصی است. خطرات بالقوه عبارتند از:

- **تأثیر بر آینده شما:** برخی از سازمانها سایت های رسانه های اجتماعی را به عنوان بخشی از بررسی پیشینه افراد استفاده میکنند. عکس ها یا نوشته های شرم آور و یا مجرمانه، مهم نیست چقدر قدیمی، می تواند مانع استخدام و یا ارتقاء شما شود. علاوه بر این، بسیاری از دانشگاه ها بررسی های مشابه برای پذیرش دانشجوهای جدید انجام میدهند. گزینه های تنظیم حریم خصوصی ممکن است شما را در این موارد محافظت نکند چون این سازمانها می توانند از شما بخواهد که صفحه آنها را «like» کنید و یا به صفحات آنها بپیوندید و یا ممکن است نوشته یا عکسی از شما در چندین سایت بایگانی شده باشد.
- **حملات علیه شما:** هکرهای سایبری می توانند پست های شما را تجزیه و تحلیل کرده و با استفاده از آنها به اطلاعات شما یا سازمانتان دسترسی پیدا کنند. به عنوان مثال، آنها می توانند اطلاعاتی که به اشتراک گذاشته اید را برای حدس زدن پاسخ به «سوالات رمزی» و تغییر رمزعبور آنلاین شما استفاده کنند، یا ایمیل های هدفمند که برای هک کردن شما تنظیم شده (spearfishing) استفاده کنند، یا با کسی در سازمان شما تماس بگیرید و تظاهر کنند که شما هستند. علاوه بر این، این حملات می توانند به دنیای فیزیکی نیز کشانده شود مانند شناسایی محل کار یا زندگی.
- **آسیب ناخواسته به کارفرما:** هکرها و یا رقبا می توانند هر گونه اطلاعات حساسی که شما در مورد کارفرما منتشر میکنید را بر علیه کارفرمای شما استفاده کنند. علاوه بر این، به طور بالقوه نوشته و گفته های شما می تواند باعث آسیب به شهرت سازمان شما شود. حتما سیاست های سازمان خود را قبل از ارسال هر چیزی در مورد کار خود مطالعه کنید، علاوه بر این برخی از پست های رسانه های اجتماعی ممکن است نظارت شود.

بهترین پیشگیری محدود کردن مطالبی است که منتشر میکنید. درست است که تنظیم گزینه های حریم خصوصی می تواند مقداری حفاظت فراهم کند، با این حال آنها اغلب گیج کننده هستند و اغلب بدون اطلاع شما تغییر میکنند. آنچه فکر می کردید خصوصی بوده ناگهان به دلایل مختلف عمومی میشوند. علاوه بر این، میزان خصوصی ماندن پست های شما به افرادی که آن را به آنها به اشتراک میگذارید دارد. هر

رسانه های اجتماعی

چه با دوستان بیشتری به اشتراک گذارید، بیشتر احتمال دارد که به اطلاعات عمومی تبدیل شوند. بطور پیش فرض هر چیزی که شما ارسال میکنید میتواند عمومی شود و بخشی دائمی از اینترنت بماند.

در نهایت، از آنچه دوستان در مورد شما ارسال میکنند آگاه باشید. اگر چیزی منتشر میکنند که شما با آن راحت نیستید، از آنها بخواهید تا آن را حذف کنند. در صورت امتناع یا نادیده گرفتن شما، با مسئولان آن سایت رسانه اجتماعی تماس بگیرید و از آنها بخواهید مطلب را برای شما از سایت حذف کنند. بطور متقابل، آنچه شما در مورد دیگران ارسال میکنید نیز رعایت کنید.




شبکه های اجتماعی سرگرم کننده با امکانات زیاد هستند، اما مراقب باشید که چه منتشر میکنید و با چه کسانی به اشتراک می گذارید.

امنیت

علاوه بر نگرانی های حریم خصوصی، در اینجا برخی از مراحل برای کمک به محافظت حساب کاربری سایتهای رسانه اجتماعی شما و فعالیت های آنلاین ذکر می شود.

- **ورود:** هر یک از حساب های کاربری خود را با یک رمز منحصر به فرد قوی حفاظت کنید و رمزها را با دیگران به اشتراک نگذارند. علاوه بر این، بسیاری از سایت های رسانه های اجتماعی خدمات احراز هویت قوی تر دارند، از جمله تأیید هویت دو مرحله ای. همیشه این روش احراز هویت قوی تر را هر زمان امکان دارد فعال کنید. در نهایت، از رسانه های اجتماعی خود برای ورود به حساب کاربری سایت های دیگر استفاده نکنید، اگر آنها هک شوند، نتیجتا تمام حساب های شما آسیب پذیر خواهند بود.
- **تنظیمات حریم خصوصی:** اگر از تنظیمات حریم خصوصی استفاده میکنید، حتما به طور منظم بررسی و آزمایش کنید. سایت های رسانه های اجتماعی اغلب تنظیمات حریم خصوصی را تغییر میدهند و احتمال اشتباه وجود دارد. علاوه بر این، بسیاری از برنامه ها و خدمات این سایتها به شما اجازه برچسب گذاری محل رخداد به محتوا را میدهند (به نام برچسب گذاری جغرافیایی). به طور منظم این تنظیمات را بررسی کنید، اگر مکان فیزیکی خود را میخواهید خصوصی نگه دارید.
- **رمزگذاری:** سایت های رسانه اجتماعی از رمزنگاری به نام HTTPS برای تامین امنیت ارتباطات آنلاین شما بکار میبرند. برخی از سایت های مانند توییتر و Google + به طور پیش فرض این امکان را فعال می سازند، در حالی که دیگر سایتها از شما میخواهند که به صورت دستی HTTPS فعال کنید. تنظیمات حساب کاربری سایت رسانه اجتماعی خود را بررسی کنید و HTTPS را به عنوان اتصال پیش فرض هر زمان ممکن است فعال کنید.
- **ایمیل:** به ایمیلهای مشکوک که ادعا می کنند از سایت های رسانه های اجتماعی آمده است مضنون باشید، اینها احتمالا جعلی و توسط هکرهای اینترنتی فرستاده شده است. امن ترین راه برای پاسخ به چنین پیامهای ورود به وب سایت های رسانه های اجتماعی به طور مستقیم است، از طریق آدرس ذخیره شده، و پس از آن خواندن و پاسخ دادن به پیام ها و یا هر گونه اعلان های وب سایت است.
- **لینک های مخرب / کلاهبرداری:** مواظب لینک های مشکوک و یا کلاهبرداری بالقوه ارسال شده در سایت های رسانه های اجتماعی باشید. خرابکاران از رسانه های اجتماعی برای گسترش حملات خود استفاده میکنند. فقط به خاطر اینکه پیامی توسط یکی از

رسانه های اجتماعی

دوستان نوشته شده به این معنا نیست که این پیام واقعا از آنهاست، ممکن است حساب هک شده باشد. اگر یکی از اعضای خانواده و یا دوستان پیامی به شما فرستاده که نمی توانید تأیید کنید (مانند اینکه از آنها سرقت شده است و نیاز به ارسال پول دارند)، با آنها از طریق تلفن همراه و یا وسایل دیگر برای تایید پیام تماس بگیرید که واقعا پیام از آنها باشد.

- **برنامه های تلفن همراه:** اکثر سایت های رسانه های اجتماعی برنامه های قابل اجرا روی تلفن همراه برای دسترسی به حساب های آنلاین شما میدهند. مطمئن شوید که این برنامه های تلفن همراه از یک سایت قابل اعتماد دانلود میکنید و گوشی های هوشمند خود را با یک رمز عبور قوی محافظت می کنید. اگر گوشی های هوشمند خود را زمانی از دست بدهید، هر کسی می تواند سایت های رسانه های اجتماعی شما را از طریق گوشی های هوشمند خود دسترسی داشته باشد و شروع به ارسال پیام از طرف شما کند.

سایت های رسانه های اجتماعی راهی فوق العاده برای برقراری ارتباط و در تماس بودن با جهان هستند. اگر راهنمایی هایی که در اینجا برشمردیم را رعایت کنید، تجربه آنلاین بسیار امن تر و لذت بخش تری خواهید داشت. برای کسب اطلاعات بیشتر در مورد چگونگی استفاده از سایت های رسانه های اجتماعی با خیال راحت و یا گزارش فعالیت های غیر مجاز، صفحه راهنمای امنیت آن سایت را مطالعه کنید.

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: http://www.securingthehuman.org

یادداشت مترجم

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

منابع

کلمات عبور:	http://www.securingthehuman.org/ouch/2015#april2015
تأیید صحت دو مرحله:	http://www.securingthehuman.org/ouch/2013#august2013
استفاده امن از برنامه های تلفن همراه:	http://www.securingthehuman.org/ouch/2015#january2015
آموزش کودکان و نوجوانان در امنیت سایبری:	http://www.securingthehuman.org/ouch/2015#june2015
امنیت فیس بوک:	https://www.facebook.com/safety

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