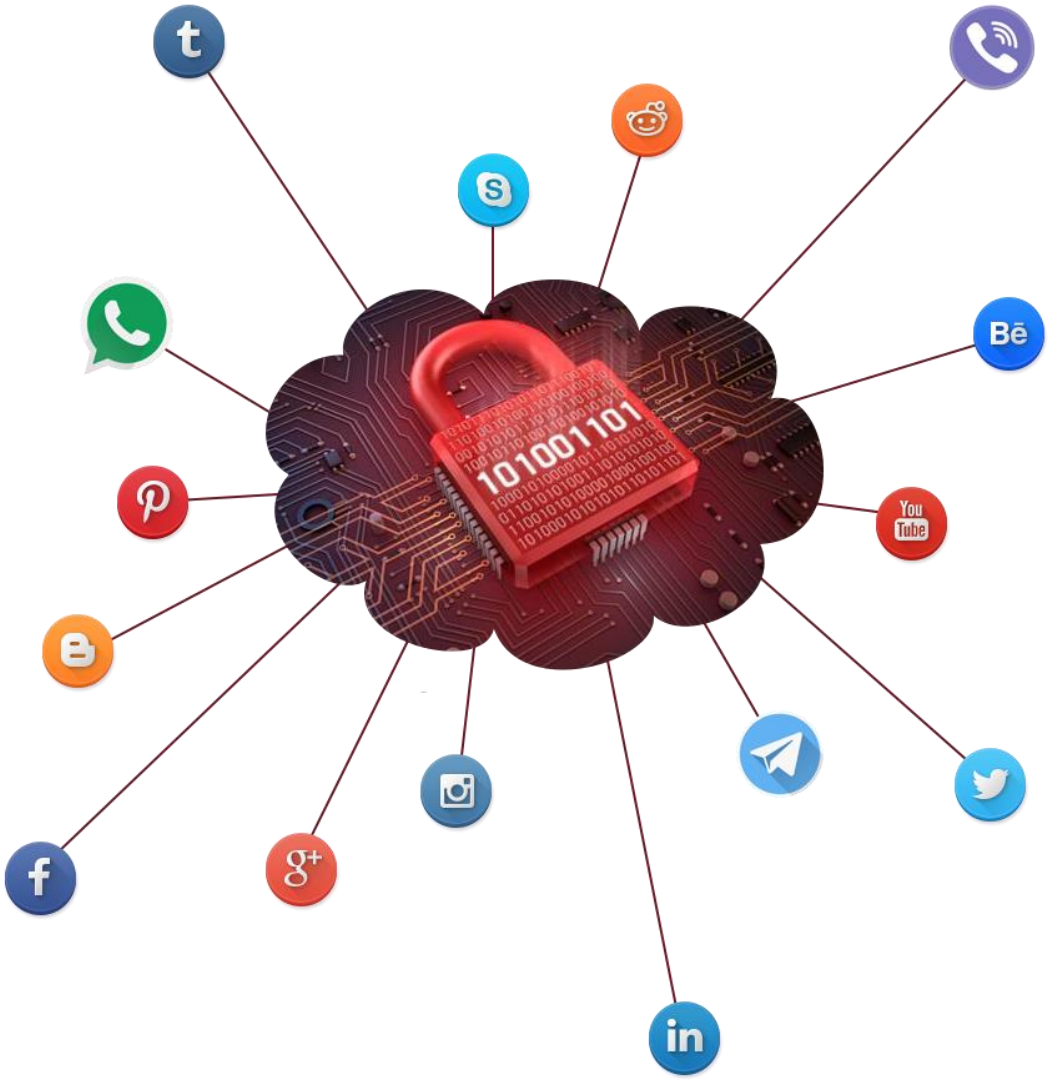

امنیت اطلاعات در شبکه های اجتماعی

مژگان شبانیان

پاییز 1394

مقدمه:

به موازات رشد بی‌سابقه استفاده از شبکه‌های اجتماعی تلفن همراه در کشور و تلاش‌های مسئولان دولتی از جمله وزارتخانه‌های ارتباطات و فناوری اطلاعات و فرهنگ و ارشاد اسلامی برای آموزش سواد رسانه‌ای در بین کاربران شبکه‌های اجتماعی، نزدیک به دو سال است که کاربران با آسیب‌های مختلفی از جمله سوءاستفاده از اطلاعات شخصی یا هجوم بدافزارهای خطرناک به تلفن همراه هوشمند یا تبلت خود روبه‌رو شده‌اند.بر همین اساس وزارت ارتباطات و فناوری اطلاعات با همکاری شرکت ارتباطات زیرساخت طرح‌های مختلفی را درباره مبارزه با آسیب‌های امنیتی فضای مجازی در دستور کار قرار داد که بسیاری از آنها در حال حاضر در مرحله اجرا قرار دارد اما نکته مهم این است که کاربران شبکه‌های اجتماعی یا فضای مجازی، نقش مهم و تعیین‌کننده‌ای در جلوگیری از حملات سایبری و تهدیدهای امنیتی دارند.

به عنوان مثال در جریان پژوهش صورت گرفته توسط روزنامه وال استریت ژورنال امریکا در سال ۲۰۱۰ میلادی از میان ۱۰۱ برنامه کاربردی محبوب کاربران تلفن همراه هوشمند، ۴۷ درصد مکان گوشی و ۵ درصد اطلاعات مربوط به سن و جنسیت را بدون آگاهی یا رضایت کاربر به اشتراک می‌گذارند، علاوه بر این، برخی برنامه‌های کاربردی محبوب تلفن همراه که داده‌ها را بدون آگاهی یا رضایت کاربران جمع‌آوری می‌کنند، آنها را در دسترس عموم قرار می‌دهند. همچنین بر اساس پژوهش صورت گرفته در سال ۲۰۱۲ توسط انجمن جهانی جی‌اس‌ام در برزیل و مکزیک، مشخص شد که بیش از نیمی از کاربران اینترنت تلفن همراه که در یک وبگاه یا برنامه کاربردی ثبت‌نام کرده‌اند، بیانیه حریم خصوصی را بدون مطالعه آن پذیرفته‌اند.

اهمیت امنیت اطلاعات

امروزه شبکه‌های اجتماعی به جزء جدایی‌ناپذیر از زندگی بسیاری تبدیل شده‌اند و حتی با وجود قابلیتهای فراوان و کاربرپسند شبکه‌های اجتماعی موجود، علاقه به راه اندازی شبکه های اجتماعی جدید با محوریتهای متفاوت و یا موضوع خاصی همواره در حال رشد است. برای مثال گروه‌های مختلف اجتماعی، از اهالی روستاها گرفته تا دانشجویان و فارغ‌التحصیلان دانشگاهی، اقدام به ایجاد شبکه های اجتماعی می کنند. اما با این وجود توجه به این نکته مهم است که تمامی این شبکه‌های اجتماعی، توسط افراد باتجربه در علوم مهندسی نرم افزار و دارای مهارت فنی کافی ایجاد نمی‌شوند. در نتیجه، چنین شبکه‌هایی عمدتا دچار ضعف‌های فراوانی در طراحی و کمبود قابلیت‌ها و ضعف‌های امنیتی هستند و در نتیجه کاربران این سامانه‌ها ممکن است با خطرات و تهدیدات متعددی مواجه شوند. براین اساس مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) موضوع امنیت شبکه های اجتماعی را از حیث طراحی و استفاده از بسته های نرم افزاری برای راه اندازی موتور این شبکه ها مورد بررسی قرار داده و نسبت به استفاده از موتورهای ناامن شبکه های اجتماعی هشدار داده است.

راه اندازی شبکه های اجتماعی به صورت سفارشی سازی شده

مرکز ماهر اعلام کرد: اگرچه برای ایجاد یک شبکه اجتماعی تخصص‌های مختلفی مورد نیاز است اما همواره نباید چرخ را از ابتدا خلق کرد. با این وجود به جهت دستیابی به یک شبکه اجتماعی می‌توان از بسته‌های نرم‌افزاری آماده تحت عنوان موتورهای شبکه اجتماعی استفاده کرد. موتورهای شبکه اجتماعی بسته‌های نرم‌افزاری هستند که برای ایجاد یک شبکه اجتماعی سفارشی‌سازی‌شده مورد استفاده قرار می‌گیرند. معمولا با استفاده از این بسته‌های نرم‌افزاری به سادگی می‌توان به یک شبکه اجتماعی دست یافت. سازوکار نصب و راه‌اندازی این موتورها مشابه سامانه‌های مدیریت محتوا (CMS) (مانند Joomla و WordPress) است که مدت‌هاست در داخل کشور به صورت گسترده برای راه‌اندازی پورتال‌ها و وب‌گاه‌ها توسط اقشار مختلف از جمله سازمان‌ها مورد استفاده قرار گرفته‌اند. موتورهای شبکه اجتماعی مختلف قابلیت‌های گوناگونی را ارائه می‌دهند؛ امکاناتی نظیر عضویت کاربر، امکان برقراری ارتباط با اعضا، درج محتوا، درج نظر بر روی محتوا، به اشتراک‌گذاری عکس، فیلم و غیره تنها بخشی از قابلیت‌های شبکه‌های اجتماعی ایجاد شده توسط این موتورها است. همچنین امکان توسعه قابلیت‌های این شبکه‌ها با استفاده از افزونه وجود دارد. بنابراین سازندگان این بسته‌های نرم‌افزاری به ملاحظاتی که از دید یک توسعه‌دهنده عادی پنهان می‌ماند، توجه کرده‌اند.

چالش های استفاده از موتورهای سفارشی برای شبکه های اجتماعی

براساس بررسی های صورت گرفته، استفاده از این موتورهای شبکه اجتماعی چالش‌هایی را نیز به همراه دارد. در صورت استفاده از این‌گونه موتورها تمام مسئولیت‌های نصب، راه‌اندازی و نگه‌داری از شبکه اجتماعی بر عهده استفاده کننده از این موتورها است. اگرچه او در تمامی امور، اختیار شبکه اجتماعی خود را دارا بوده و تمامی اطلاعات کاربران محفوظ خواهد ماند. در همین حال باید گفت سازندگان شبکه های اجتماعی سفارشی سازی شده به علت عدم اطلاع کافی از بسترهای سخت‌افزاری مورد نیاز برای اجرای مناسب شبکه اجتماعی، از بسترهای ضعیف استفاده کرده و یا بیش از اندازه برای بستر سخت‌افزاری هزینه می کنند. مرکز ماهر تاکید کرد: اگرچه در طراحی و پیاده‌سازی موتورهای شبکه اجتماعی معمولا به امنیت توجه ویژه شده است اما در صورت استفاده از آن‌ها، فراهم کردن امنیت از جهاتی دشوارتر نیز می‌شود چرا که این موتورها در دسترس عموم قرار داشته و هکرها در سرتاسر دنیا تمامی زوایای کد آن‌ها را با هدف یافتن یک آسیب‌پذیری بررسی و تحلیل می‌کنند. به‌عنوان مثال چندی پیش یکی از شبکه‌های اجتماعی که از موتورهای شبکه اجتماعی بهره برده بود، هک شده و اطلاعات دو میلیون کاربر آن در اختیار هکرها قرار گرفت.

کاهش امنیت شبکه های اجتماعی به دلیل کمبود اطلاعات فنی

در نتیجه کشف آسیب‌پذیری‌های موتورهای شبکه اجتماعی از سوی هکرها، سازندگان این موتورها به صورت پیوسته نسخه‌های جدیدتری را که آسیب‌پذیری‌های کشف شده در آن‌ها رفع شده است، منتشر می‌کنند. بنابراین کاربران این موتورها باید پیوسته دغدغه به روزرسانی موتور شبکه اجتماعی خود را داشته باشند که در بسیاری از موارد این‌چنین نیست و در این صورت دچار چالش‌های جدی امنیتی خواهند شد. چالش بعدی نیز این است که برخی از طراحان شبکه های اجتماعی و کاربران موتورهای این شبکه ها به علت کمبود اطلاعات فنی ممکن است این موتورها را به گونه‌ای مناسب پیکربندی نکرده و در نتیجه کاربران نهایی در حین استفاده با مشکلات مختلفی از جمله کاهش سرعت پردازش، کاربرپسندی و از همه مهم‌تر کاهش امنیت وب‌گاه مواجه شوند. با این وجود به طراحان شبکه های اجتماعی داخلی توصیه می شود که در بکارگیری موتورهای راه اندازی این شبکه ها جوانب احتیاط امنیتی را رعایت کنند و کاربران نهایی نیز در عضویت در این شبکه ها با آگاهی بیشتری عمل کرده و اطلاعات مهم و شخصی خود را در این شبکه ها قرار ندهند.

راه های برای ایمن ماندن در شبکه های اجتماعی

کارشناسان امنیت سایبری برای ایمن ماندن کاربران در شبکه های اجتماعی چندین عامل مهم را در نظر گرفته اند که در ادامه به معرفی این عوامل پرداخته ام.

1.سیستم عاملی انتخاب کنید که رمزگذاری را پشتیبانی کند

به مشترکان موبایلهای هوشمند توصیه می شود که اگر واقعا به امنیت دستگاه موبایل خود اهمیت می دهند باید از سیستم عامل و دستگاه موبایلی استفاده کنند که رمزگذاری مبتنی بر سخت افزار را برای حافظه های داخلی و خارجی پشتیبانی می کند.

این به این معنا است که داده های ذخیره شده بر روی موبایل کاربر در برابر پیشرفته ترین هکرها نیز تا حد بالایی محافظت می شود چرا که بدون رمزگذاری ممکن است فردی بتواند داده های موجود بر روی دستگاه را حتی بدون در اختیار داشتن PINیا کلمه عبور نیز بازیابی کند.

2.برای گوشی خود یک PIN یا کلمه عبور انتخاب کنید

فعال کردن یک کلمه عبور یا PIN نخستین خط دفاعی برای محافظت از محرمانه ماندن و امنیت گوشی های موبایل تلقی می شود؛ این اقدام به کاربر کمک می کند تا در صورت گم شدن، به سرقت رفتن و یا جا ماندن گوشی در جایی، از برداشتن آن توسط دیگران و مشاهده و دستکاری در محتویات آن جلوگیری به عمل آید. معمولا در صورتی که رمزگذاری بر روی دستگاه فعال باشد، انتخاب کلمه عبور برای آن یک اجبار است.

اگر رمزگذاری توسط سیستم عامل پشتیبانی نشده باشد، کاربر باید حتما خود را ملزم به تعیین یک کلمه عبور مناسب برای دستگاه خود بداند. زیرا اگرچه احتمالا داده های کاربر توسط افراد خاصی که کلمه عبور را نیز ندارند قابل بازیابی است، اما حداقل به این شکل این اطلاعات در برابر برخی مجرمان محافظت خواهد شد.

3.از بین بردن خودکار اطلاعات را فعال کنید

اغلب سیستم عاملهای موبایل، حذف خودکار اطلاعات دستگاه را پس از چند بار تلاش ناموفق برای وارد کردن کلمه عبور، پشتیبانی می کنند. این کار در صورتیکه رمزگذاری توسط دستگاه پشتیبانی نشده باشد، بسیار ارزشمند است، اما برای دستگاههایی که از رمزگذاری بهره می برند نیز می تواند مفید باشد. دادن فرصت نامحدود به دیگران برای حدس زدن کلمه عبور، احتمال کشف آن را بیشتر می کند.

4.ردیابی و مدیریت از راه دور را فعال کنید

پیش از آنکه گوشی یا دستگاه موبایل کاربر گم شده یا به سرقت رود، باید راهکار ردیابی و مدیریت از راه دور برای آن تنظیم شود. اغلب این راهکارها به کاربر اجازه می دهد که موقعیت دستگاه را بر روی یک نقشه مشاهده کند و این باعث می شود که هشدارهای صوتی برای کمک به پیدا کردن گوشی ارسال و با نمایش یک پیغام تصویری به دیگران می گوید که چگونه گوشی را به کاربر بازگردانند.

این راهکارها همچنین به کاربران اجازه می دهد که از راه دور موبایل خود را قفل کرده و یا داده های آن را پیش از دستیابی دیگران به آن، پاک کند.

5.استفاده از Wi-Fi hotspot ها را محدود کنید

زمانی که کاربر از Wi-Fi hotspot هایی استفاده می کند که رمزگذاری شده نیستند، تمامی ترافیک اینترنت کاربر از طریق بی سیم منتقل شده و به راحتی می تواند مورد نفوذ قرار گیرد.

مهمترین وب سایتها و سرویسها مانند وب سایتهای بانکی، معمولا رمزگذاری (HTTPS/SSL)خود را پیاده سازی می کنند که از ترافیک آنها محافظت می کند اما اغلب ارائه دهندگان سرویسهای ایمیل و بسیاری از شبکه های اجتماعی این کار را انجام نمی دهند؛ در نتیجه شنود کنندگان احتمالا می توانند کلمات عبور و ترافیک مربوط به این وب سایت ها را جمع آوری کنند.

باید توجه داشت که نسل سوم، نسل چهارم موبایل و اغلب ارتباطات داده ای سلولی دیگر، معمولا توسط بستر ارتباطی رمزگذاری می شوند. علاوه بر این استراق سمع بر روی این نوع از ارتباطات چندان معمول نیست براین اساس کاربر باید تا جایی که می تواند سعی کند به جای Wi-Fi hotspot های ناامن از ارتباطات داده ای استفاده کند.

اما در صورتیکه کاربر اصرار به استفاده از Wi-Fi hotspot ها دارد باید از آنهایی استفاده کند که رمزگذاری و احراز هویت را فراهم می آورند.

6.از یک آنتی ویروس یا برنامه امنیتی استفاده کنید

ویروسها، بدافزارها و هک برروی دستگاههای موبایل کم کم در حال تبدیل شدن به یک مسئله بزرگ است و با این وجود کاربر باید یک برنامه امنیتی نصب کند تا بتواند از آلودگی و نفوذ جلوگیری کند.

اغلب راهکارهای آنتی ویروس، ویژگیهای دیگری را نیز در اختیار کاربر قرار می دهند که از آن جمله می توان به حذف اطلاعات از راه دور، پشتیبان گیری و تعیین موقعیت مکانی گوشی اشاره کرد.

ده راهکار اولیه برای عدم سو استفاده از اطلاعات شخصی

یکی دیگر از مشکلاتی که ممکن است کاربران شبکه های اجتماعی موبایلی با آن رو به رو شوند،سوء استفاده از مشخصات کاربری و اطلاعات شخصی توسط افراد مختلف است،کارشناسان برای این مسئله که از اهمیت بالایی هم برخوردار است ده راهکار ارائه کرده اند که این راهکار ها در ادامه ذکر شده است.

1.گمنام ثبت نام کنید

اول از همه یک ایمیل جدید درست کنید. از هیچ یک از مواردی که باعث شناختن هویت شما می شود (از جمله نام و نام خانوادگی، سال تولد یا کد پستی) در آدرس ایمیل جدید یا پروفایل تان استفاده نکنید. با استفاده از این آدرس ایمیل جدید، صفحات رسانه‌ای اجتماعی را ایجاد کنید و فقط افرادی را که واقعا به آنها اعتماد دارید اضافه کنید. همچنین از گذاشتن عکس های شخصی که به شناسایی شما کمک می‌کند اجتناب کنید.

2.از رمز عبورهای قوی استفاده کنید

پسورد هایتان را برای اکانت هایی که دارید به روز رسانی کنید و مطمئن شوید که برای هر کدام از اکانت هایی که دارید پسورد قوی استفاده کرده‌اید. برای ساختن یک پسورد قوی می توانید از ترکیب حروف (حداقل یک حرف بزرگ) و عدد استفاده کنید، به خاطر داشته باشید که می توانید از کاراکتر های خاص (از جمله @ # $ ٪ !) نیز استفاده کنید. از رمز عبورهایی که به راحتی قابل حدس زدن هستند به هیچ وجه استفاده نکنید.

3.تنظیمات حریم خصوصی خودتان را ارتقاء دهید

هر رسانه‌ی اجتماعی، گزینه ای برای تنظیمات دارد که در آن به شما اجازه می‌دهد امنیت حساب کاربری خود را افزایش دهید. بنابراین با استفاده از آن شما می‌توانید فقط به دوستانتان یا افراد خاصی اجازه بدهید که پست های شما و اطلاعات شخصی‌تان را ببینند. هیچ وقت تصور نکنید که تنظیمات پیش‌فرض، به صورت محرمانه تنظیم شده است.

4.از شناسه‌های مکان‌یابی استفاده نکنید

تنظیمات مکان‌یابی را خاموش کنید و هرگز اطلاعات مکانی را که در آن می خواهید باشید (مثلا هنگام خارج شدن از شهر برای تعطیلات) را به اشتراک نگذارید. حتی مشخصات مکانی که معمولاً برای خرید کردن به آنجا می روید را با دیگران در میان نگذارید. این کار باعث می شود که مردم کارهای روزمره ای را که انجام می دهید پیدا کنند و درنتیجه می توانند مکانی را که شما قرار است به آنجا بروید پیش‌بینی کنند.

5.افرادی را که به عنوان دوست قبول می کنید، با دقت انتخاب کنید

مطمئن شوید افرادی که شما را به عنوان دوستی اضافه می‌کنند را می شناسید. قبل از اینکه درخواست دوستی را قبول کنید یک پیام خصوصی برای آن شخص بفرستید و از او چیزی را درخواست کنید که به شما در شناساندن هویتش کمک می کند. حتی اگر شما فرض کنید که می توانید او را از روی عکس یا نام تشخیص دهید، در این صورت برای شما راحت تر خواهد بود که بفهمید این فرد همان شخصی است که می شناسید یا اینکه نقش او را بازی می کند (این روش، یکی از روش های مرسوم برای جعل هویت است).

6.اطلاعات شخصی‌تان را به اشتراک نگذارید

منظور از این اطلاعات، مواردی همچون شماره‌های بیمه اجتماعی، تاریخ تولد، شماره تلفن واطلاعات بانکی است. سارقین هویت می توانند از این اطلاعات شما استفاده کنند. اگر فردی از لحاظ قانونی به این اطلاعات شما نیاز داشته باشد، راه‌های دیگری نیز وجود دارد که می تواند با استفاده از آنها با شما تماس بگیرد.

7.ارسال کردن ، دوباره ارسال کردن، لایک کردن

هیچ چیزی بر روی اینترنت به طور کامل امن نیست. هر کسی می تواند آنچه را که شما پست کرده‌اید ذخیره کند و یا اینکه آن را با دیگران به اشتراک بگذارد. پس به خاطر داشته باشید چیزی را که می خواهید ارسال کنید با دقت بیشتری انتخاب کنید. همیشه فرض کنید چیزی

را که ارسال می کنید باقی خواهد ماند و حذف نمی شود. هیچ وقت چیزی را درمورد خودتان،خانواده تان یا دوستان تان، که خود شما یا آنها دوست ندارند عمومی شود را ارسال نکنید. همیشه از ارسال چیزهایی که لحظه ای به ذهنتان خطور می‌کند اجتناب کنید، و اینکه از ارسال چیزی که باعث پشیمانی و تأسف خوردن شما می شود خودداری کنید.

8.از عکس‌ها و آبروی‌تان محافظت کنید

اگر شخصی چیزی را ارسال کرده است که شما آن را دوست ندارید به آنها اجازه بدهید که بدانند این برای شما ناخوشایند است و از آنها درخواست کنید که آن را بردارد. به صورت منظم بخش "عکس هایی مربوط به خود" را چک کنید و ببینید که چه کسی آن را ارسال کرده است، همچین دیوار (wall) خودتان را بررسی کنید و چیزهایی که در آن برچسب خورده‌اید را ببینید. اگر فردی از حذف کردن چیزی که برای شما ناخوشایند است امتناع می کند، پس ضروری است تا او را بلاک کنید و یا اینکه آن را گزارش (report) کنید.

9.مراقب چیزی که بر روی آن کلیک می کنید باشید

اگر بر روی لینک هایی که از محتوای آن خبر ندارید کلیک کنید، آگاه باشید که هکرها می توانند با استفاده از این روش وارد اکانت شما شوند و یا اینکه می توانند ویروسی را از طریق آن پخش کنند. اگر فردی چیزی را برای شما ارسال کرد و این فایل غیر طبیعی به نظر برسد و یا اینکه برای شما ناآشنا باشد، یک پیام برای آنها ارسال کنید و از آنها در مورد این فایل توضیح بخواهید و به آنها این فرصت را بدهید که فکر کنند که شما می دانستید آنها قصد هک کردن شما را داشتند.

10. شناخت کامل از کاری که می‌خواهید انجام دهید را داشته باشید

اگر شما توسط کسی اذیت شدید، مکالمه یا پست آزارگر را ذخیره کنید و یا از آن یک عکس (اسکرین شات) بگیرد و آن را به سایت مربوطه و یا هر شخصی که با چنین موقعیت هایی سرو کار داشته باشد (مانند وکیل، مشاور، و یا مددکار اجتماعی) گزارش دهید.

نتیجه

همه ی ما دوست داریم ساعاتی را در روز در شبکه های اجتماعی مثل Twitter و Facebook بگذرانیم ما همچنین ممکن است صرف نظر از تفریح و به دلایل حرفه ای و جدی تر از این سایت ها استفاده کنیم.اما شبیه به خیلی از چیزهای دیگر در اینترنت ، این شبکه های اجتماعی خطرات خاص خود را دارند که ممکن است با رعایت نکردن نکات امنیتی برای ما دردسر ساز شوند و تلافی ساعات خوش ما را در این سایت ها درآورند.

هکرها می توانند از طریق رسانه های اجتماعی به اطلاعات شخصی شما دست پیدا کنند و یا ویروس (به اصطلاح malware) های مورد نظرخود را وارد سیستم شما کنند و شما را مورد آزار و اذیت قرار دهند.این اتفاقات ممکن است حتی تا جایی پیش بروند که شهرت و اعتبار و موقعیت شغلی شما و درنهایت زندگی شما را نشانه بروند و آن ها را نابود کنند.

پس شما نیاز دارید تا در شبکه های اجتماعی ایمن بمانید.اقدامات ایمنی را دنبال کنید و مطمئن باشید زندگی اجتماعی آنلاین شما ، ضد اجتماعی نخواهد شد، اقداماتی از قبیل:

- گمنام ثبت نام کردن
- استفاده از رمز های قوی
- تنظیمات حریم خصوصیمان را ارتقا بدهیم
- عدم استفاده از شناسه های مکان یاب
- پذیرش دوستان در دنیای مجازی باید با شناخت و دقت صورت بگیرد
- عدم اشتراک گذاری فایل های شخصی
- هیچ وقت لینک هایی که از محتوای آن اگاه نیستید را باز نکنید.

مراجع:

1. علی احمدی، تبیان : افزایش امنیت در شبکه‌های اجتماعی، 1393/12/11
http://www.tebyan.net/newindex.aspx?pid=295878
2. آرش کریم‌بیگی، ایستنا : ضعف‌های امنیتی در موتورهای شبکه‌های اجتماعی/ هک اطلاعات کاربران– 24 آذر 1394
http://www.ictna.ir/id/075009/
3. روزنامه دنیای اقتصاد : 6 نکته برای حفظ امنیت موبایل – 21 شهریور 1392
http://www.donya-e-eqtesad.com/news/751254/
4. علی عیدی، زومیت : 10 راه حل ساده برای ایمن ماندن در شبکه های اجتماعی – 7 تیر 1394
http://www.zoomit.ir/howto/web/21613-social-network-security
5. دانیال حجاری، زوم تک : حفظ امنیت در شبکه های اجتماعی زیر ذره بین زوم تک
http://zoomtech.ir/security-in-social-networks-zoomtech/

تهیه شده توسط تیم مقاله آی تی

www.it-research.ir