فضای تاریک دنیای وب

موضوع این مقاله : حریم خصوصی و امنیت سایبری

نویسنده : محسن امیری فخر

درباره نویسنده

محسن امیری فخر

- کارشناس ارشد نرم افزار از دانشگاه شهید بهشتی
- طراح و تحلیلگر سیستم های مبتنی بر وب
- متخصص شبکه های کامپیوتری، تحلیلگر سیستم و کارشناس فضای مجازی، ابری و کلیه امور مرتبط با سئو
- مسلط به MCSE 2016 ، Kerio Control ، HTML5 ، CSS3 ، ASP.net ، DNN
  TMG ، Lync Server ، Exchange Server
- مسلط به نرم افزار Photoshop – مسلط به زبان انگلیسی
- طراح گرافیک و تهیه کننده فیلم های واقعیت مجازی VR 360

www.linkedin.com/in/mohsenamirifakhr

Mohsen.Amiri.Fakhr@gmail.com

www.Mamiri.ir , www.MohsenAmiri.ir

Tel : +989126758683 - +982146023141

آبرو در لغت

- آبرو در لغت به‌معنای ناموس و شرف و اعتبار و ... آمده و انسان به‌خاطر کرامت ذاتی که دارد جانشین خداوند متعال در روی زمین شده و از طرفی فرشتگان هم مأمور به سجده کردن برای انسان شدند تا جایی‌که اباکننده از آن از درگاه الهی رانده شد. بنابراین نفس این انسان محترم است و شایسته احترام .

آبرو از دیدگاه پیامبر اعظم (ص)

- یامبر اکرم(ص) درباره اهمیت این موضوع می‌فرمایند: «همه چیز مسلمان، از مال، آبرو و خونش بر مسلمان دیگر حرام است. هرگاه مؤمن برادر دینی خود را متهم نماید، ایمان او آب می‌شود و از بین می‌رود همان طوری که نمک در آب حل می‌شود و از بین می‌رود».
- امام صادق(ع) نیز در جایی به نقل از رسول خدا(ص) فرمودند: خداوند تبارک و تعالی امر کرده است: «هر کس دوستی از دوستان مرا خوار کند، در کمین جنگ با من نشسته است».
- در حدیث دیگری از پیامبر اسلام(ص) آمده است که فرمودند: «وقتی پروردگارم عزَّوجلّ مرا بالا برد(در معراج) به قومی گذشتم که ناخن‌های مسین داشتند و صورت و سینه خویش را می‌خراشیدند، گفتم ای جبرئیل این‌ها چه کسانی هستند؟ گفت: اینان آن کسانی‌اند که گوشت مردم خورند و از عرض و آبرویشان سخن کنند».

آبرو از دیدگاه امام صادق (ع)

- امام صادق(ع) می‌فرمایند: کسی‌که به‌منظور عیب‌جویی و ریختن آبروی مؤمن و این‌که او را از نظر مردم بیندازد سخنی را نقل کند، خداوند او را از ولایتش بیرون کرده، به‌سوی ولایت شیطان می‌فرستد ولی شیطان هم او را نمی‌پذیرد. از نظر اسلام حفظ جان، مال و آبروی مردم و حتی اندیشه آنان محترم است و ریختن آبروی مؤمن بسیار خطرناک و گناه بزرگی به‌شمار می‌رود به همین دلیل است که امام صادق(ع) در حدیثی، فرموده است: «المؤمن اعظم حرمه من الکعبه» حرمت مؤمن را از حرمت کعبه بالاتر دانستند. اما متأسفانه گاهی دیده می‌شود در جامعه اسلامی حرمت و آبروی اشخاص حفظ نمی‌شود و با سادگی آبروی مسلمانی را می‌برند و هیچ توجهی به عقاب دنیوی و اخروی آن ندارند.

آبروی مؤمن به مثابه تمام سرمایه و اعتباری است که در طول زندگی با سختی آن را به‌دست آورده است.

چکیده

- چرایی این مورد که چرا اساسا باید همچین نوشته ایی از خود به عنوان متخصص فضای مجازی ارائه دهم و در واقع چه نقصانی در این سیستم بسیار پیچیده که مشابه یک ابر سیاه و تاریک میتواند همه چیز را در خود جای دهد دیده ام ، که لزوم آنرا برخود میبینم که در این فضا، اندکی برای شما از نقصان و ضعف این فضا بنویسم.

مقدمه

فضای مجازی در جهان دارای دو جنبه اصلی و بزرگ است : جنبه اول همین فضای معمولی می باشد که ما به عنوان مخاطبان عادی به کسب و کار ، تجارت ، تفریح و ... می پردازیم .

جنبه دوم : فضایی به نام Dark Web می باشد که غالبا از آن به عنوان جنبه تاریک فضای وب نام می برند ، همان فضایی که هکرها برنامه نویسان مخرب و ... درفضای مجازی در تلاش برای آسیب زدن به روال عادی زندگی در فضای سالم و سفید برای منافع گاها سودجویانه چه اقتصادی ، چه سیاسی و چه شخصی و شخصیتی مثل **ترور شخصیت افراد** ... و تخریب افراد مختلف و دارای هویت در این فضا

موضوع اصلی این نوشته : در حقیقت بررسی این نوع واکنش ها از نوع ترور شخصیت و افراد دارای هویت در فضای مجازی ست که متاسفانه نویسنده این مقاله نیز از این مورد در امان نبوده است .

در ادامه با کمک از وبسایت باشگاه خبرنگاران جوان و وبسایت کودک و اینترنت به بررسی راهکارهای امنیت سایبری خواهیم پرداخت.

این مقاله از نوع مقاله های گرد آوری شده از منابع مختلف می باشد

وضع فعلی رعایت حریم شخصی در دنیای وب

- متاسفانه در دنیای فضای وب چه ایران و چه خارج از ایران جنبه های احترام به حریم شخصی افراد ، جنگ رودرو ، رعایت ادب و آبروی افراد تنها در حد چند نظریه ساده باقیمانده و اساسا گردانندگان اصلی فضای وب با رصد روزانه ایی که از ایمیل ها ، پیام ها و موارد دیگر دارند هیچ علاقه ایی به احترام به موارد مذکور ندارند
- شاید یکی از اصلی ترین دلایل این عدم رعایت حریم شخصی ، ضعف حقوقی می باشد که متاسفانه در فضای کنونی وجود دارد و صد البته درکشور عزیزمان بخاطر عدم وضع قوانین مربوط کپی رایت شاید از وضع کنونی جهانی نیز عقبتر باشیم .

جنبه های ترور شخصیت در دنیای وب

- همه ما معنی ترور شخصیت را می دانیم !!
- در این مقاله نمیخواهیم ترور شخصیت را با هم به بحث بگذاریم
- از آن طرف که یکی از اصلی ترین ابزارهای ترور شخصیتی افراد و یا نفوذ به خصوصی ترین حریم های آنها خود فضای مجازی است اساسا باید بگوییم ترور شخصیت جزعی لاینفک از کلیات فضای وب را تشکیل داده است .
- متاسفانه به اشکال مختلف در فضای مجازی افراد سودجو با هر پیشینه و هدفی قصد تخریب افراد با هویت مشخص و حتی نامشخص برای جذب منافع بیکران که گاها مالیست می باشند
- برای آنها وزیر ، وکیل ، استاد دانشگاه و رفتگر و ... فرقی نمی کند
- هدف این دسته افراد تنها رسیدن به سود مورد نظر می باشد

تعریف حریم خصوصی

- به زبان ساده می‌توان گفت (حریم خصوصی) از آن دست مفاهیمی است که همه آنرا می فهمند و درک می‌کنند لکن نمی‌توانند تعریفی جامع و کامل از آن ارائه نمایند لذا در بسیاری موارد ما شاهد نوعی تعارض و یا حتی چالش در زمینه مسائل مربوط به حریم خصوصی هستیم به طور مثال زمانی سخن از نصب دوربین‌های مدار بسته در کافی نتها به میان آمده بود که مخالفین این طرح آنرا معارض با حریم خصوصی افراد می‌دانستند و برخی دیگر همچون نگارنده این مطلب آنرا غیرمرتبط با حریم خصوصی افراد تلقی می‌کردند.
- چنین اختلافاتی بعضا ناشی از آن است که تعریف ترمینولژیکی از (حریم خصوصی) ارائه نشده است لکن در مجموع می‌توان بیان نمود: حریم خصوصی یعنی (فرد آزادانه حق داشته باشد در خلوت خود اطلاعات مربوط به امور زندگی‌اش را پنهان نموده و بر آن کنترل داشته و مانع دسترسی دیگران به این اطلاعات گردد و تصمیم بگیرد که چه وقت و تا چه حد این اطلاعات را به دیگران منتقل نماید).

- در تعالیم دینی نیز به بشر آموزش داده می‌شود که برای زندگی خود حریمی خصوصی قائل شود و از افشاء اطلاعات زندگی‌اش خودداری نماید آنجا که امام معصوم می‌فرماید چند چیز خود را از دیگران پنهان نما: اینکه چقدر مال داری؟ اینکه کجا می‌روی؟ و اینکه مشرب فکری و مذهب تو چیست؟

نقض حریم خصوصی در فضای مجازی

- تا اینجا دانستیم که انسان به حکم طبیعت و سرشت باید دارای حریم خصوصی برای خود باشد و از آن محافظت نماید در مقابل افراد بایستی نسبت به صیانت و رعایت حریم خصوصی سایرین اقدام نمایند. نقض حریم خصوصی در فضای مجازی یکی از مهمترین مسائل روز جامعه ماست که از دو منظر قابل بررسی است یکی از جانب قربانیان نقض حریم خصوصی در فضای مجازی و دیگری از سوی ناقضین حریم خصوصی در فضای مجازی.

- بزه دیدگان در فضای مجازی نقش مهمی را در بروز جرایم ناقض حریم خصوصی ایفا می کنند و در عین حال می توانند در اقدامات پیشگیرانه علیه جرایم سایبری یا همان نقش آفرین باشند. بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می شود،استعدادی قابل توجه برای قربانی شدن بروز می‌دهند و براحتی طعمه بزهکاران سایبری می‌شوند برخی کلاهبرداری‌های اینترنتی ناشی از کسب اطلاعات به روشهای بسیار ساده و سوء استفاده از عکسها و اسرار شخصی نمونه هایی از این موضوع می‌باشد.

- ضعف شخصیتی. فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و ... مواردی است که قربانی بزه سایبری را در قربانی شدنش مساعدت می‌کند. افراد بایستی نسبت به صیانت از حریم خصوصی خود همت نمایند، بسیاری افراد بدون رعایت مسائل امنیتی، خصوصی‌ترین اطلاعات خود را بر روی سیستم رایانه‌ای و یا حامهای داده نظیر فلش و کارتهای حافظه و تلفن همراه و سی‌دی و ... ذخیره نماید و به نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند و اینچنین استعداد قربانی شدن در فضای مجازی را از خود نشان می‌دهند.

مصادیق نقض حریم خصوصی در فضای مجازی

جنبه دیگر موضوع همانطور که معروض گردید مربوط به ناقضان حریم خصوصی در فضای مجازی است. این بزهکاران زمانی که وارد فضای مجازی یا همان اینترنت می‌شوند در خیالی خام آنرا (ملک طلق) خود دانسته و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود می‌دهند.

- **در زیر به برخی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه ای جرم انگاری شده است می‌پردازیم:**

۱- دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت افراد

۲- شنود غیرمجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم افزارهای شنود چت‌های اینترنتی.

۳- دسترسی غیرمجازبه داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن.

۴- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت.

۵- نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده.

۶- حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده بطور غیرمجاز.

۷- از کار انداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی بطور غیرمجاز نظیر غیرفعال سازی دیتابیس تارنماها و ممانعت از دسترسی افراد به سایتهای شخصی.

۸- ممانعت از دسترسی اشخاص مجاز به داده های یا سیستمهای رایانه ای یا مخابراتی بطور غیرمجاز.

۹- ربودن داده‌های متعلق به دیگری بطور غیرمجاز.

۱۰- هتک حیثیت از طریق انتشار صوت و فیلم تحریف شده دیگری بوسیله سیستم‌های رایانه‌ای یا مخابراتی.

۱۱- نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی.

۱۲- فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.

۱۳- آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی.

حفظ حریم خصوصی در شبکه های اجتماعی

- امروزه اینترنت در سرتاسر دنیا بسیار فراگیر شده است. تا این لحظه تعداد کاربران اینترنت در سراسر جهان در حدود ۳.۶ میلیارد نفر هستند. تعداد سایتهای ثبت شده در اینترنت به ۱.۲ میلیارد میرسد و این حجم از کاربران روزانه در حدود ۲۰۰ میلیارد ایمیل ارسال میکنند، ۴ میلیارد جستجوی گوگل انجام میدهند، ۶ میلیارد ویدئو در یوتیوب مشاهده میکنند، ۶۰ میلیون عکس در اینستاگرام به اشتراک میگذارند و نزدیک به یک میلیارد توئیت انجام میدهند. جالب است بدانید که به صورت میانگین در حدود ۴ میلیارد گیگابایت اطلاعات به صورت روزانه در اینترنت جابجا می‌شود. این آمارها نشان از میزان نفوذ اینترنت در دنیا دارد .
- شبکههای اجتماعی بر ابعاد مختلف زندگی فردی و اجتماعی افراد و در سطح کشورها و حتی بین‌الملل تاثیر میگذارند، به همین دلیل روز به روز در حال گسترش هستند و در آینده نیز، نقش به مراتب بیشتر و مهم‌تری را در زندگی اجتماعی افراد بازی خواهند کرد.
- یکی از نگرانیهای اساسی در مورد اینترنت، حفظ حریم شخصی افراد است. اطلاعات گوناگونی که درباره اشخاص در اینترنت قرار داده می‌شود، امکان نقض حریم خصوصی افراد را به شدت افزایش می‌دهد.
- ظهور شبکه ها به معنای تهدید بزرگ‌تر حریم اطلاعات و رابطه‌ای افراد، در مقایسه با شکل‌های قدیمی‌تر ارتباطات است. این تهدید ناشی از دسته‌بندی و ادغام اطلاعات درباره هر شخص و قابلیت ردگیری کارهای روزانه اوست. این به معنای بوجود آمدن ارزشی ضد ارزش به نام در دسترس بودن در هر مکان و زمان است که می‌توان رد افراد را تا عمیق‌ترین زوایای جامعه گرفت.

حریم خصوصی کاربران در شبکه های اجتماعی

یک شبکه ی اجتماعی متشکل از گروهی از افراد و تعاملات بین آنها است. بنابراین شبکه های اجتماعی را می‌توان محیطی دانست که از طریق آنها افراد مختلف می‌توانند با استفاده از فضای مجازی به تعامل با یکدیگر پرداخته و از طریق آن اطلاعات خود را با دیگران به اشتراک بگذارند. شبکه های اجتماعی با وجود نوظهور بودن، به سرعت رشد کرده و امروزه صدها شبکهی اجتماعی مختلف در حال فعالیت در سراسر دنیا هستند.

- حفظ حریم خصوصی افراد در شبکه های اجتماعی یکی از مهارتهای مهمی است که کاربران باید از آن آگاه باشند. بعضی از افراد بدون هیچگونه توجهی اطلاعات و داده‌های شخصی خود را به اشتراک میگذارند. حتی شناختن دوستان و فالورها هم دلیل خوبی برای این بی‌دقتیها نیست، زیرا عواقبی در پی دارد که گاها جبران ناپذیرند.

بررسی مخاطرات شبکه‌های اجتماعی

- با وجود نوظهور بودن شبکه های اجتماعی مجازی، امروزه صدها شبکهی اجتماعی متنوع به وجود آمده است. هر کدام از این شبکه‌ها فرصت‌ها و تهدیدهای خاص خود را دارد که با استفاده درست از آن‌ها می‌توان در عین حفظ حریم خصوصی از مزایای بیشمار آن‌ها نیز بهره برد.

❑ نقض حریم خصوصی

- همه روزه تعداد کاربران شبکه های اجتماعی رو به افزایش است و از آنجایی که بیشتر آنها چیز زیادی درباره حفاظت از حریم خصوصی خود نمی‌دانند و یا با وجود اینکه می‌دانند به آن اهمیتی نمی‌دهند، اطلاعات شخصی و حساس خود را به راحتی در اختیار دیگران قرار میدهند. نگرانی اصلی زمانی بوجود می‌آید که علی‌رغم ایجاد برخی سیاستهای محرمانگی از سوی شبکه های اجتماعی مختلف، همچنان این شبکه ها آسیبپذیر هستند. در اینجا ذکر این نکته ضروری است که در اکثر موارد این نفوذها با استفاده از غفلت کاربران و بی احتیاطی خود آن‌ها در استفاده از این شبکه ها، صورت می‌گیرد. حمله‌کنندگان می‌توانند اطلاعات حساس افراد را بدست آورده و مورد سوءاستفاده قرار دهند. آمارها و آزمونهای مختلف برای بررسی کاربران شبکه های اجتماعی نشان میدهد که اغلب کاربران بسیاری از اطلاعات مهم و خصوصی خود را در این شبکه ها قرار داده و بدون هیچ شناخت و تحقیقی پیشنهادهای دوستی را میپذیرند. که خب این یکی از پرخطرترین کارهاست. (Liuو همکاران، ۲۰۰۸)

بررسی حفظ حریم خصوصی و راهبردهای امنیت سایبری

- امروزه اینترنت و شبکه های اجتماعی به بخشی از زندگی ما تبدیل شده‌اند. هر فرد به طور متوسط چندین ساعت از زمان خود را در این شبکه ها سپری کرده و به گفتگو و تبادل اطلاعات با دیگران میپردازد. با در نظر گرفتن این شرایط، لازم است تا ما به طور دقیق نسبت به حریم خصوصی خود حساس بوده و اقدامات لازم را به منظور افزایش حریم خصوصی و امنیت دیجیتالی خود به کار بندیم. این بخش، آشنایی با روش‌های امنیتی در شبکه های اجتماعی و روشهای حفظ حریم خصوصی فرد و اطرافیان او را ارائه می‌کند، که با به کار بستن آن‌ها می‌توانیم محیط این شبکه‌ها را برای خود و اطرافیانمان امن‌تر کنیم.(چترودی و اخذمی، ۱۳۹۴)

❑ مکانیزم های تأیید هویت شبکه های اجتماعی

- بسیاری از اپراتورهای شبکه های اجتماعی تلاش میکنند که با فعال کردن اقدامات امنیتی مانند مکانیسم تایید هویت کاربر و یا تنظیمات حریم خصوصی، از کاربران خود محافظت کنند. تعدادی از این روشها در ادامخ بیان شده است: (باطنی و ترک، ۱۳۹۵)
- • مکانیسم احراز هویت: به منظور اینکه اطمینان حاصل شود که آیا کاربری که ثبت نام می‌کند یک کاربر واقعی است یا یک کاربر جعلی یا یک حساب کاربری خطرناک؛ اپراتورهای OSNاز مکانیسم تایید هویت استفاده می‌کنند. این روش‌ها شامل شناسایی عکس دوستان، تصدیق هویت چند فاکتور، یا در بعضی مواقع درخواست از کاربر است؛ که یک کپی از نام کاربری خود را ارسال کند. بعنوان مثال تلگرام دو عامل مکانیسم احراز هویت را معرفی کرده است، کاربر زمان وارد شدن به تلگرام نه تنها نیاز به وارد کردن رمزعبور دارد، بلکه یک کد تایید به تلفن همراه او ارسال می‌شود که باید آن را نیز وارد نماید. این مکانیسم باعث می‌شود که از ورود کاربر با یک حساب کاربری جعلی جلوگیری شده و اطلاعات نادرست منتشر نشود. این روش از حوادث گوناگونی مانند زمانی که یک هکر یک حساب تلگرام را میرباید، جلوگیری می‌کند و در نهایت باعث حفظ حریم افراد می‌شود زیرا از دسترسی افراد غریبه به مکالمات خصوصی و گروهی شما در تلگرام جلوگیری می‌کند.

بررسی حفظ حریم خصوصی و راهبردهای امنیت سایبری

- تنظیمات امنیت و حریم خصوصی: بسیاری از شبکه های اجتماعی آنلاین از تنظیمات حریم خصوصی کاربر با قابلیتهای مختلف پشتیبانی می‌کنند. کاربران فیسبوک می‌توانند تنظیمات حریم خصوصی خود را سفارشی کنند و کاربران قادر خواهند بود که مشاهده مطالب، تصاویر، نوشته ها و سایر بخش‌های حساب خود را شخصی سازی کنند. لازم است بدانیم که در هر کدام از این شبکه‌ها به روشی می‌شود امنیت را بالابرد مثلا در Googleکاربران می‌توانند دوستان خود را به گروه‌های متفاوتی مثل دایره بهترین دوستان، دایره دوستان مدرسه، دایره کار و ... دسته‌بندی کنند. در ادامه بیشتر درباره این روش‌های حفاظتی صحبت خواهیم کرد.
- • مکانیسمهای حفاظت داخلی: بعضی از شبکه های اجتماعی کاربران خود را با اجرای مکانیسمهای حفاظت داخلی اضافی در برابر اسپم، پروفایلهای جعلی، کلاهبرداری و سایر تهدیدات حفاظت می‌نمایند، تا امنیت و البته حریم خصوصی آن‌ها به بهترین نحو حفظ شود. برای مثال فیسبوک از کاربران خود در برابر حملات مخرب و جمعآوری اطلاعات بوسیله فعال کردن سیستم ایمنی فیسبوک (FISمحافظت می‌کند.
- • گزارش کاربران: یکی از روشهایی که اپراتورها می‌توانند از طریق آن از کاربران جوان و نوجوان خود در برابر آسیبها محافظت کنند، دریافت گزارش است. در این روش، اپراتورها یک گزینه به منظور گزارش سوءاستفادهها و یا سیاستهای نقض شده در شبکهی خود قرار داده و از این طریق کاربران در صورت مشاهدهی این موارد، بلافاصله به اپراتورها اطلاع خواهند داد، تا برخورد لازم صورت بگیرد و در صورت لزوم حساب کاربری فرد خاطی مسدود شود.

بررسی حفظ حریم خصوصی و راهبردهای امنیت سایبری

اصول استفاده از شبکه های اجتماعی

- به هنگام استفاده از شبکه های اجتماعی با رعایت تنها چند اصل ساده به راحتی می‌توان از وقوع بسیاری از اتفاقات جلوگیری نموده و تا حد زیادی از آسیب‌های این شبکه‌ها و نقض حریم خصوصی در امان ماند. در ادامه برخی از این اصول به طور خلاصه ذکر شده است (بشیر و همکاران، ۱۳۹۲):.
- • فراموش نکنید که اینترنت همیشگی است: داده‌ای که شما در فضای آنلاین منتشر میکنید، برای همیشه آنجا خواهد ماند. مهم نیست که شما آن داده را پاک کنید. حتی پاک کردن اکانت شما نیز منجر به پاک کردن آن نخواهد شد. آنچه که شما منتشر میکنید برای همیشه توسط دیگران قابل دسترسی خواهد بود. بنابراین همیشه دقت کنید که چه اطلاعاتی را در اینترنت منتشر میکنید.
- • همیشه در کلیک کردن لینکها احتیاط کنید: مهم نیست چه کسی آن لینک را ارسال کرده باشد. حتی اگر ارسال کننده دوست شما باشد، بدون احتیاط بر روی لینکها کلیک نکنید. دزدان اینترنتی از شبکه های اجتماعی برای دزدیدن اطلاعات شما، از این لینک‌ها استفاده میکنند، چون به این وسیله فریب دادن شما راحتتر است. آنها از اکانت دوستان شما استفاده میکنند تا لینکهای خطرناک را برای شما ارسال کنند. کافیست تا شما بر روی آن لینکها کلیک کنید تا اطلاعات خصوصی شما به دست آنها بیفتد. بنابراین همیشه مواظب لینکها باشید.
- • در پذیرفتن دوستی افراد بسیار دقت کنید: هرگز به عکس و اسم افرادی که به شما درخواست دوستی میدهند اعتماد نکنید. از کجا میدانید که این اطلاعات واقعی است؟ در شبکه های اجتماعی، استفاده از عکس و نام قلابی بسیار ساده و مرسوم است. تنها دوستی کسانی را بپذیرید که آنها را در دنیای واقعی میشناسید.
- • مرتبا تنظیمات مربوط به حریم خصوصی خود را چک کنید: همهی شبکه های اجتماعی تنظیماتی برای حریم خصوصی دارند. مطمئن شوید که این تنظیمات به گونهای قرار داده شده است که اطلاعات شما را تنها با دوستان و خانوادهی شما در میان میگذارد. همچنین مرتبا در بازه های زمانی مشخص این تنظیمات را مجددا بررسی کنید، تا در صورت تغییر آنها در اسرع وقت متوجه شوید.

بررسی حفظ حریم خصوصی و راهبردهای امنیت سایبری

- هرگز اطلاعات شخصی خود را منتشر نکنید: در انتشار اطلاعات شخصی (مانند آدرس خانه، شماره تلفن، شماره ملی و شناسنامه و غیره) بسیار دقت کنید. هرگز این اطلاعات را در محیط مجازی منتشر نکنید. این‌ها شخصی‌ترین اطلاعات شما هستند و نیاز است برای حفظ حریم خصوصی شما، محرمانه باقی بمانند. اگر کسی این اطلاعات را از شما پرسید، به او شک کنید. این اطلاعات می‌تواند به سادگی به دزدان اینترنتی امکان دزدیدن اطلاعات شما را بدهد.
- رمز عبور خود را مرتبا عوض کنید: هرگز رمز عبورهایی را انتخاب نکنید که به سادگی قابل حدس زدن باشند. رمز عبوری، انتخاب کنید که حداقل ۸ کاراکتر داشته باشد و متشکل از عدد، حروف و علامتها باشد. رمزهای عبور خود را در بازه های زمانی (مثلا هر ۶ ماه) عوض کنید. برای اکانتهای مختلف هرگز یک رمز عبور یکسان استفاده نکنید.
- مراقب باشید اطلاعات شما در کجا منتشر می‌شوند: دقت کنید که ممکن است شبکه های شما به هم متصل باشند. مثلا ممکن است عکسی که شما در توئیتر منتشر میکنید به طور خودکار در فیسبوک نیز منتشر شود.

بررسی حفظ حریم خصوصی و راهبردهای امنیت سایبری

- هرگز در سفر موقعیت جغرافیایی خود را به اشتراک نگذارید: در مواقعی که به مسافرت میروید هرگز مکان جغرافیایی خود را به همراه عکسهای خود به اشتراک نگذارید. اینگونه شما به دزدان نشان میدهید که خانه ی شما آماده ی سرقت است. زمانی عکسها و مناطق را به اشتراک بگذارید که به خانه بازگشتهاید.
- همیشه در زندگی آنلاینتان همانند زندگی واقعی حد و مرزی برای ارتباطاتتان قائل شوید: قبل از آنکه متنی را در گروه‌های تلگرامی قرار دهید یا چیزی را در اینستاگرام منتشر کنید، کمی تأمل کنید و ببینید آیا کسی از دیدن آن آزرده نخواهد شد و یا اینکه در آینده برایتان مشکلی ایجاد نمیکند؟ به عنوان یک اصل، همیشه چیزی را منتشر کنید که کسی در آینده نتواند آن را دست مایه‌ی سوءاستفاده از شما قرار دهد.
- حواستان باشد که لیست دوستانتان شامل چه کسانی است: حتی مراقب دوستانِ دوستانتان باشید، ممکن است آنها هم برایتان مشکل ساز شوند. ممکن است شما تنها به دوستانتان اجازهی دیدن پستها و عکسهای فیس‌بوکتان را داده باشید، اما وقتی که دوستی برای شما کامنت میگذارد و یا مطلبتان را لایک میکند، آنگاه دوستان او هم قادر به دیدن مطلب شما هستند. به عنوان مثال شما عکسی خانوادگی را برای لیست خانوادهی خود به اشتراک میگذارید. هیچ کسی جز اعضای خانوادهی شما در این لیست قرار نداشته و قاعدتا نباید بتواند عکس شما را مشاهده کند. برادر شما که در لیست خانواده قرار دارد، عکس شما را لایک می‌کند و این امر باعث می‌شود تا یک فرد غریبه که در لیست دوستان برادر شما است، از طریق همین لایک به عکس شما دسترسی پیدا کند. این مشکلات یادآور یک اصل مهم خواهد بود، اصلی که همواره لازم است رعایت کنید تا دچار مشکل نشوید: «هیچگاه چیزی را که از انتشار آن در زندگی واقعیتان احساس امنیت و راحتی نمیکنید، در فضای مجازی منتشر نکنید، زیرا سرانجام کسانی که نباید، آن را خواهند دید.»

بررسی حفظ حریم خصوصی و راهبردهای امنیت سایبری

- هرگز در سفر موقعیت جغرافیایی خود را به اشتراک نگذارید: در مواقعی که به مسافرت میروید هرگز مکان جغرافیایی خود را به همراه عکسهای خود به اشتراک نگذارید. اینگونه شما به دزدان نشان میدهید که خانه ی شما آماده ی سرقت است. زمانی عکسها و مناطق را به اشتراک بگذارید که به خانه بازگشتهاید.
- همیشه در زندگی آنلاینتان همانند زندگی واقعی حد و مرزی برای ارتباطاتتان قائل شوید: قبل از آنکه متنی را در گروه‌های تلگرامی قرار دهید یا چیزی را در اینستاگرام منتشر کنید، کمی تأمل کنید و ببینید آیا کسی از دیدن آن آزرده نخواهد شد و یا اینکه در آینده برایتان مشکلی ایجاد نمیکند؟ به عنوان یک اصل، همیشه چیزی را منتشر کنید که کسی در آینده نتواند آن را دست مایه‌ی سوءاستفاده از شما قرار دهد.
- حواستان باشد که لیست دوستانتان شامل چه کسانی است: حتی مراقب دوستانِ دوستانتان باشید، ممکن است آنها هم برایتان مشکل ساز شوند. ممکن است شما تنها به دوستانتان اجازهی دیدن پستها و عکسهای فیس‌بوکتان را داده باشید، اما وقتی که دوستی برای شما کامنت میگذارد و یا مطلبتان را لایک میکند، آنگاه دوستان او هم قادر به دیدن مطلب شما هستند. به عنوان مثال شما عکسی خانوادگی را برای لیست خانوادهی خود به اشتراک میگذارید. هیچ کسی جز اعضای خانوادهی شما در این لیست قرار نداشته و قاعدتا نباید بتواند عکس شما را مشاهده کند. برادر شما که در لیست خانواده قرار دارد، عکس شما را لایک می‌کند و این امر باعث می‌شود تا یک فرد غریبه که در لیست دوستان برادر شما است، از طریق همین لایک به عکس شما دسترسی پیدا کند. این مشکلات یادآور یک اصل مهم خواهد بود، اصلی که همواره لازم است رعایت کنید تا دچار مشکل نشوید: «هیچگاه چیزی را که از انتشار آن در زندگی واقعیتان احساس امنیت و راحتی نمیکنید، در فضای مجازی منتشر نکنید، زیرا سرانجام کسانی که نباید، آن را خواهند دید.»

نتیجه گیری و جمع بندی

سایتهای شبکه های اجتماعی آنلاین می‌تواند خدمات مؤثر و سرگرم کننده‌ای را برای کاربران، با به اشتراک گذاری علاقهمندیهای خود و ارتباط با دوستان صرف نظر از محدودیتهای جغرافیایی و اقتصادی، فراهم کنند. در عین حال این شبکه ها می‌توانند کاربر را در معرض خطر جدی امنیت سایبر قرار دهد. درک روشنی از مسائل مربوط به امنیت در شبکه های اجتماعی می‌تواند به کاربر کمک کند تا چگونگی کاهش خطرات نقض حریم خصوصی را فرا گیرد.

- امروزه دیگر گشت و گذار در وب، سفر یک نفره و مکاشفه در تنهایی نیست، زیرا شبکه های اجتماعی از قبیل اینستاگرام، تلگرام و غیره، به بخش جدایی ناپذیری از فرهنگ زندگی آنلاین تبدیل شده‌اند. در کنار آن هرجا تعداد کاربر زیاد می شود، توجهی افراد سوءاستفاده‌گر را هم به خود جلب میکند. برای همین، این شبکه ها در حال تبدیل شدن به حفره‌های مهم امنیتی هستند که هر روزه کاربران بی‌احتیاط زیادی را در کام خود فرو میبرند.
- همانطور که روز به روز استفاده افراد از شبکه های اجتماعی از قبیل فیس‌بوک، اینستاگرام و تلگرام بیشتر و بیشتر میشود، حفظ حریم خصوصی نیز اهمیت بیشتری پیدا میکند. عضویت در شبکه های اجتماعی در مواردی منجر به مشکلاتی شده است. کم نیستند افرادی که از برچسب خوردن عکسهایشان توسط دیگران و یا دیده شدن عکسهای خصوصیشان توسط دوستان نه چندان صمیمی شاکیاند. در برخی جوامع این مشکل به اندازه‌ای زیاد شده که کلماتی مانند Facebook Friend به فرهنگ لغات هم راه یافته‌اند و دوستان فیسبوکی را از دوستان واقعی جدا کرده‌اند.
- توصیه ما برای کاربران شبکه های اجتماعی این است که اطلاعات غیر ضروری را حذف کنند، حریم خصوصی و امنیتی خود را تنظیم کنند. بهتر است که کاربران شبکه های اجتماعی مانند اینستاگرام صفحه‌های شخصی خود را خصوصی کرده و اطلاعات خود را فقط در معرض دید خانواده و دوستان واقعی خود قرار دهند. بهتر است که درخواست دوستی افراد ناشناس را رد کنند. نصب حداقل یکی از نرم‌افزارهای امنیتی تجاری را انجام دهند و همواره به یاد داشته باشند که هیچ چیز هرگز از روی اینترنت پاک نخواهد شد.

سخن آخر با دوست عزیزی که در فضای مجازی ادعای زرنگی می کند :

دوست عزیزی که در حال کنکاش زندگی مردم ، اسکرین شات گرفتن از پیام های شخصی خود با دیگران و نشان دادن آن در فضای مجازی و بردن آبروی آنها !! خواهشمندم اندکی خود را در دنیای آخرت فرض نموده البته به صورت مجازی در پیشگاه حضرت حق ، شاید که اصلاح شوید .

فضای مجازی هیچگاه پاک از بدی ها نمی شود ، اما ما تلاش کنیم آلوده به فضای تاریک آن نشویم

با سپاس از وبسایت باشگاه خبرنگاران جوان و وبسایت کودک و اینترنت

و در نهایت سپاس از شما خواننده محترم ...

محسن امیری فخر

۰۹۱۲۶۷۵۸۶۸۳

Mohsen.Amiri.Fakhr@gmail.com

www.Mamiri.ir