فصلنامه دانش انتظامی سمنان ، دوره نهم ، شماره سی و دوّم ، تابستان ۱۳۹۸

تاریخ دریافت مقاله: ۱۳۹۷/۱۱/۰۱

تاریخ بازنگری نهایی مقاله: ۱۳۹۸/۰۳/۱۸

تاریخ پذیرش مقاله: ۱۳۹۸/۰۵/۱۳

صفحات: ۶۴ - ۵۱

حریم خصوصی در فضای مجازی

علی گرزالدین [۱*]، حسین صادقی کاشان [۲]

چکیده

شبکه‌های اجتماعی تحولی عظیم در به اشتراک‌گذاری اطلاعات و تعاملات اجتماعی مجازی درکشورمان به وجود آورده‌اند با وجود اینکه هر روز بر تعداد کاربران در شبکه‌های اجتماعی افزایش پیدا می‌کند حفظ حریم خصوصی در میان کاربران برای شرکت‌های ارائه دهنده خدمات به کاربران به یک نگرانی بدل شده است.

به طور کلی افزایش تعداد کاربران شبکه‌های اجتماعی باعث ایجاد رخنه‌های امنیتی درشبکه‌های اجتماعی شده است. سرقت هویت، نظارت و تحکیم سایبر، بهره‌کشی از کودکان تنها برخی از مشکلاتی هستند که به وجود آمده‌اند که این اتفاقات نشان می‌دهد حریم خصوصی به طور کامل توسط شبکه‌های اجتماعی حمایت نمی‌شود که باعث نگرانی کاربران این شبکه‌ها شده‌اند.

امروز ما می‌توانیم در هر زمان به هرگونه اطلاعات مربوط به هر کسی از هر نقطه دسترسی داشته باشیم اما این تهدید جدیدی برای اطلاعات خصوصی و محرمانه کاربران است. شکسته شدن حریم خصوصی افراد ازهر قشر و رده‌ای، باعث ناامنی روانی و اجتماعی می‌شود و می‌تواند پیامدهای جبران‌ناپذیری به همراه داشته است. هدف از این پژوهش علاوه بر شناخت خدماتی که به عنوان شبکه اجتماعی در فضای مجازی ارائه می‌شود و دسته‌بندی انواع آنها، بررسی مفهوم حریم خصوصی در فضای مجازی و نقاط چالش برانگیز از جهت نقض حریم خصوصی در شبکه‌های اجتماعی است.

واژگان کلیدی: اینترنت، شبکه‌های اجتماعی، حریم خصوصی.

---

[۱]- (نویسنده مسئول) ----------@----------

[۲]- کارشناس ارشد حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی

مقدمه

شبکه های اجتماعی رسانه ای جدیدهستند که افراد را به مبادله ایده ها، ارتباط با دیگران و... را دراختیار کاربران قرار داده است. شبکه های اجتماعی موانع ارتباطی را از بین برده و کانال ارتباطی غیر متمرکز را ایجاد کرده اند .

شبکه های اجتماعی مزایای زیادی را به همراه آورده است، به ما اجازه می دهد به راحتی با دوستان و خانواده در سراسر جهان ارتباط برقرار کنیم، به ما اجازه می دهد که مرزهای بین المللی را از بین ببریم. این شبکه ها تأثیر منفی بر زندگی ما دارند، زیرا ترکیبی از انزوا و دسترسی جهانی فرهنگ ما را از بین می برد.

شبکه های اجتماعی اعتماد به نفس ما را تحت تاثیر قرار داده وتوانایی ما را از خودکفایی درفکر کردن به طور مستقل می گیرد و به جای آن باعث می شود که ما آرامش بخشی برای پیوستن به هر گروه ای که پیام های ناسازگارانه ای را بشنویم که گوش ما را گول زده و حواس ما را بدون ارزیابی پیامدهای آن تحریک کنیم.

در واقع شبکه های اجتماعی به طرز وحشیانه ای ما را تبدیل به یکی از نسل های ضد اجتماعی می کنند،

هنوز. ما پیام کوتاه را برای مکالمه تلفنی، چت آنلاین به صورت جلسه رو به رو ترجیح می دهیم ولی این شبکه ها بسیاری از تعاملات افراد را با سیستم عامل های مناسب مانند فیس بوک، توییتر و Instagram جایگزین کردند.

به طور واضح تاثیرات منفی شبکه های اجتماعی را می توان در سه دسته اصلی نشان داد. .

اولا، شبکه های اجتماعی، احساس غلطی از "ارتباطات" آنلاین و دوستی های سطحی را که منجر به مشکلات عاطفی و روانی می شود، را افزایش می دهد.

دومین آسیب شبکه های اجتماعی این است که می تواند به راحتی اعتیاد آوربوده وباعث از دست رفتن زمان شده زمانی که متعلق به فرد و خانواده بودن است که این امر موجب کاهش مهارت های بین فردی شده ومنجر به رفتار ضد اجتماعی می شود.

سرانجام، رسانه های اجتماعی ابزارهایی برای جنایتکاران، شکارچیان و تروریست ها به شمار می آیند که به آنها امکان اعمال مجازات را می دهد

تجزیه و تحلیل سوم شامل نشان دادن ارتباط بین مشکلات روانی ناشی از رسانه های اجتماعی و فعالیت های جنایی است.

طرح مسئله

حریم خصوصی از مباحث مهم و عام اخلاق است که در حوزه اخلاق حرفه ای به ویژه اخلاق پژوهش چالش های فراوانی را به میان آورده است. امروزه فن آوری اطلاعات ، ذخیره سازی اطلاعاتی را ممکن ساخته است که در گذشته جز با انبارهایی بزرگ از پرونده های قطور ممکن نبوده است امروزه فن آوری اطلاعات ، بازیابی اطلاعاتی را میسور ساخته که در گذشته یا ممکن نبوده ویا بسیار مشکل بوده است .

خیلی جالب است شما در منزل خود نشسته اید و کالایی حجیم را از آن سوی دنیا خریداری کنید وچند روز بعد درب منزل تحویل بگیرید اینها اموری است که فن آوری اطلاعات در اختیار بشر قرار داده است .هرچه فن آوری اطلاعات پیشرفت می کند امکان فریب کاری و تقلب های انسانی نیز ابعاد جدیدتری پیدا می کند.درزمینه تاثیرات فن آوری اطلاعات برحریم خصوصی ،مقالات و کتب زیادی به نگارش در امده است برخی سوالات این بحث عبارت است از :حریم خصوصی چیست و لازم است چه حد آن از سوی افراد دیگر، حرمت نهاده شود؟ نهاد ها چه وظایفی در باب حفظ حریم خصوصی افراد دارند؟آیا دولتها می توانند حریم خصوصی افراد را نقض کنند؟.

فرضیه ها

- شبکه های اجتماعی عاملی برای نقض حریم خصوصی کاربران
- استفاده مجرمین سایبری از شبکه های اجتماعی و محصولات این فناوری در راستای اهداف مجرمانه خود ونقض حریم خصوصی

تعریف حریم خصوصی

اگر بخواهیم حریم خصوصی را تعریف کنیم، می‌شود گفت یعنی یک فرد یا گروه بتواند خود و یا اطلاعات مربوط به خود را مجزا کند و در نتیجه بتواند خود و یا اطلاعاتش را با انتخاب خودش در برابر دیگران آشکار کند.

مرزها واطلاعات آنچه که خصوصی در نظر گرفته می شود، در میان فرهنگ ها و افراد متفاوت است، اما موضوعات مشترک را به اشتراک می گذارند. وقتی چیزی برای یک فرد خصوصی است، معمولا این بدان معنی است که چیزی به لحاظ ذاتی خاص یا حساس به آن است. دامنه حریم خصوصی بخشی از امنیت (محرمانه بودن) است که می تواند شامل مفاهیم استفاده مناسب و همچنین حفاظت از اطلاعات باشد.

حریم خصوصی در سطح بین المللی به عنوان حقوق بشر در ابعاد مختلف به رسمیت شناخته شده است.

- حریم شخصی
- حریم شخصی رفتار شخصی
- حفظ حریم شخصی ارتباطات
- حفظ اطلاعات شخصی.

حریم خصوصی کاربران در شبکه های اجتماعی

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

اینترنت و حریم خصوصی

یکی از نگرانی های اساسی در مورد استفاده کنندگان فضای مجازی، حفظ حریم شخصی کاربران است. نگرانی های مربوط به حفظ حریم خصوصی از ابتدای به اشتراک گذاری رایانه در مقیاس بزرگ بیان شده است.

اینترنت وسیله ارتباطی جدید و پویا به سرعت از محیط دانشگاهی وارد عرصه عمومی شده و یکی از سرویسهای آن لاین بی شماری است که در زمینه ارتباطات انقلابی ایجاد کرده است.

افراد و سازمانهای سراسر دنیا از این وسیله برای مقاصد ارتباطی تفریحی آموزشی و... استفاده می برند و به عنوان «بزرگترین شکل مشارکتی گفتار جمعی که تاکنون شناخته شده»معرفی شده است. اینترنت همانند یک محل مجازی ملاقات عمومی شهروندان جهان و شبکه شبکه ها و بزرگترین شبکه جهانی رایانه است.

یکی ازدلایل اصلی موفقیت اینترنت تبادل اطلاعات در سراسر جهان است اما این آزادی اغلب باعث ایجاد مشکل برای کسانی می شود که اطلاعات با ارزشی را در اینترنت منتقل می کنند این اطلاعات می تواند اطلاعات حساس درباره کاربران باشد که می تواند بدون هیچ رد و پا و به طور الکترونی جا به جا کرد.

بنابراین یکی از نگرانیهای اساسی در مورد اینترنت حفظ حریم شخصی افراد است اطلاعات گوناگون که درباره داده ها نگهداری می شود از طریق نفوذ به این سیستم ها امکان سوء استفاده و ایجاد خطر را برای شهروندان به دنبال دارد.

تعریف شبکه های اجتماعی

شبکه اجتماعی شامل اتصال اشخاص و سازمان های گوناگون با وابستگی های مختلف می باشد. این وابستگی ها می تواند شامل دوستی، رابطه خویشاوندی و علایق مشترک باشد. در واقع شبکه های اجتماعی برای اتصال میان خانواده، دوستان و همکاران ، در راستای اشتراک محتواهای گوناگون همچون عکس، اطلاعات، شایعات و اخبار و رویدادهای روز به کار می روند در تعریفی دیگر از شبکه های اجتماعی آمده هدف ازوبسایت شبکه اجتماعی ایجاد جامعه ای برخط از کاربران اینترنتی است که امکان درهم شکستن موانع گوناگون زمانی، مکانی و اختلافات فرهنگی را فراهم می سازد. در واقع شبکه های اجتماعی امکان تعامل میان افراد گوناگون را توسط اشتراک گذاری عقاید فراهم می سازد .

در تعریفی دیگر آمده شبکه اجتماعی شکلی از , سلایق، اطلاعات و تجربیات به صورت برخط فراهم می نماید

جامعه ای برخط بوده که افراد گوناگون با علایق، فعالیت ها، و پیش زمینه های مشترک را گردهم می آورد. اغلب این شبکه ها بر پایه (Heidemann) وب بوده و امکان بارگزاری متن، تصویر و فیلم و تعامل میان کاربران را به شیوه های گوناگون برقرار می نماید. (semnan n.d.)

حفظ حریم خصوصی افراد در شبکه های اجتماعی یکی از مهارت های 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 بی‌دقتی ها نیست، زیرا عواقبی در پی دارد که گاها جبران ناپذیرند.

مصادیق نقض حریم خصوصی در شبکه‌های اجتماعی

در طول سالیان، جرائم رایانه‌ای در فضای مجازی ابعاد بسیار گسترده‌ای مانند کلاه‌برداری‌های اینترنتی، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، جعل داده‌ها و عناوین، تجاوز به حریم خصوصی اشخاص و گروه‌ها، سرقت اطلاعات، هرزه‌نگاری و جرائم اخلاقی و برخی جرائم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی یافته که لزوم ایجاد پلیس تخصصی که توان پی‌جویی و رسیدگی به این‌چنین جرائم سطح بالای فناورانه را داشته باشد، بیش‌ازپیش برجسته ساخته است.

از سوی دیگر با تصویب قانون جرائم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات کمیسیون فضای تبادل اطلاعات (فتا) دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، این بخش در بهمن‌ماه سال ۱۳۸۹ به دستور فرماندهی نیروی انتظامی جمهوری اسلامی ایران، تشکیل شد.

قانون جرائم رایانه‌ای در سال ۱۳۸۸ برای تعیین مصادیق استفاده مجرمانه از سامانه‌های رایانه‌ای و مخابراتی به تصویب مجلس شورای اسلامی رسید و به دنبال آن کمیته تعیین مصادیق محتوای مجرمانه بر اساس ماده ۲۲ این قانون تشکیل و پس‌ازآن فهرستی از مصداق‌های محتوای مجرمانه توسط این کمیته در دی‌ماه ۱۳۸۸ ارائه شد.

این فهرست در ۵ فصل در بخش‌های «محتوای خلاف عفت و اخلاق عمومی، محتوای علیه مقدسات، محتوای علیه امنیت و آرامش عمومی، محتوای علیه مقامات و نهادهای دولتی و عمومی و محتوایی که برای ارتکاب جرائم رایانه‌ای و سایر جرائم» تهیه‌شده است که عنوان قانون جرائم رایانه‌ای گرفت. علاوه بر بخشی از این فهرست که در قانون مجازات اسلامی نیز آمده است، در برخی موارد نیز که معلول جرائم جدید به وجود آمده به دلیل فضای منحصربه‌فرد مجازی است مصادیق تازه‌ای ارائه شد و برای آن‌ها جرم و مجازات تعریف شد.

قوانین مرتبط با رعایت حریم خصوصی در کشور

توجه به حریم خصوصی یکی از ارکان حقوق شهروندی در هر جامعه¬ای است و افراد جامعه باید آگاهی¬های لازم در مورد این حق را داشته باشند.

یکی از مهم‌ترین عوامل ایجاد آرامش ذهنی مردم و امنیت روانی جامعه توجه و حفاظت از حریم خصوصی توسط تمامی بخش‌های کشور و ایجاد بستری مناسب برای برخورد با ناقضان حریم خصوصی است. با گسترش وسایل ارتباطات جمعی و فضای مجازی و ایجاد و توسعه شبکه‌های اجتماعی توجه به حریم خصوصی اهمیتی مضاعف یافته و مرز میان حریم خصوصی و عمومی هرروز باریک¬تر می‌شود.

ازاین‌رو نیاز به قوانین و مقررات پیشگیرانه که با مجازات سنگین و بدون اغماض، با ناقضان حریم خصوصی و افشاگران اسرار مردم برخورد کند امری مشهود در این حوزه است. البته اجرای صحیح این کار، مشروط به آموزش مردم، بیان مصادیق حریم خصوصی و نقض آن و فرهنگ‌سازی در این زمینه است تا بتوان هم خلاهای قانونی را رفع کرد و هم راهکارهایی ارائه داد تا یکی از مهم‌ترین مقوله‌های حقوق شهروندی مردم که حفظ حریم خصوصی آن‌ها است، نهادینه شود و هر کس منطبق با شرایط و موقعیت اجتماعی خود، حداقل آگاهی و دانش را در رابطه با حریم شخصی خود و دیگران داشته باشد.

البته در سال‌های اخیر، اقداماتی برای حفظ حریم خصوصی افراد جامعه و مجازات خاطیان در این زمینه انجام‌شده که بسیار مؤثر بوده است. بااین‌حال تلاش‌های بیشتری توسط متولیان امر برای گسترش قوانین بازدارنده در این زمینه موردنیاز است.

مصداق نقض حریم خصوصی در شبکه‌های اجتماعی

در سال‌های اخیر تلاش‌های زیادی در مورد اهمیت بخشی بیشتر به لزوم رعایت حریم خصوصی افراد در فضای مجازی را شاهد بوده‌ایم. این سیاست‌ها با تدوین و تصویب حقوق شهروندی که حفظ حریم خصوصی یکی از ارکان آن است نمود عینی یافته است. بااین‌حال این قوانین نیازمند نظارت و التزام دستگاه‌های گوناگون و برقراری هماهنگی‌های لازم برای اجرا است که امید می‌رود به‌زودی شاهد رشد و گسترش مفاهیم حقوق شهروندی در همه ابعاد باشیم.

یکی از مهم‌ترین بخش‌های موجود در قانون جرائم رایانه‌ای حوزه مرتبط با نقض حریم خصوصی و انجام فعالیت‌های بزهکارانه در فضای مجازی است.

مصادیق نقض حریم خصوصی در شبکه‌های اجتماعی که در قانون (به‌ویژه قانون جرائم رایانه‌ای) جرم‌انگاری شده، به شرح زیر است:

۱. دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا حساب کاربری اشخاص

۲. شنود غیرمجاز محتوای در حال انتقال در سیستم¬های رایانه‌ای یا مخابراتی نظیر استفاده از نرم‌افزارهای شنود چت‌های اینترنتی

۳. دسترسی غیرمجاز به داده‌های سری در حال انتقال در سیستم¬های 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 به‌قصد دسترسی به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده

۶. حذف یا تخریب یا مختل یا غیرقابل‌پردازش کردن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده به‌طور غیرمجاز

۷. از کار انداختن یا مختل کردن سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز نظیر غیرفعال سازی پایگاه‌داده تارنماها و ممانعت از دسترسی اشخاص به پایگاه‌های اینترنتی شخصی

۸. ممانعت از دسترسی اشخاص مجاز به داده‌های یا سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز

۹. ربودن داده‌های متعلق به دیگری به‌طور غیرمجاز

۱۰. هتک حیثیت از طریق انتشار یافتن صوت و فیلم تحریف‌شده دیگری به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی

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

۱۲. فروش یا انتشار یافتن 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 جرائم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی

بررسی حفظ حریم خصوصی

امنیت سایبری به هیچ وجه مسئله ای ثابت با راه حل دائمی نیست. تهدیدات برای اطلاعات در فضای مجازی سریعا تکامل یافته و اخیرا به کانال های جدید مانند رسانه های اجتماعی و فن آوری های تلفن همراه گسترش یافته است. همانطور که سازمان ها در تلاش هستند تا با چشم انداز در حال تغییر ایجاد شده توسط فن آوری های نوآورانه، شیوه های اجتماعی و تهدیدات همیشه در حال تغییر باشند، اطلاعات تولید شده، جمع آوری شده و جمع آوری شده در مقیاس وسیع می تواند آسیب پذیر باشد به تهدیدات اینترنتی. در زیر برخی از چالش های در حال ظهور برای حفاظت از داده ها و امنیت سایبر است.

در رسانه های اجتماعی، حریم خصوصی دیگر انتخاب شخصی نیست بعضی افراد ممکن است فکر کنند که حریم خصوصی آنلاین، به خوبی، موضوع خصوصی است. اگر شما نمی خواهید اطلاعات خود را خارج از اینترنت کنید، آن را در رسانه های اجتماعی قرار ندهید. ساده، درست است؟

شبکه های اجتماعی به شدت تغییر کرده است که افراد چگونه با دوستان، همکاران و اعضای خانواده خود ارتباط برقرار می کنند. اگر چه شبکه های اجتماعی مثل توییتر، فیس بوک، +Google، YouTube، Snapchat و

FourSquare نقش مهمی در زندگی روزمره ما ایفا می کنند، آنها همچنین می توانند خطرات جدی درمورد حفظ حریم خصوصی ایجاد کنند. هنگام استفاده از این سایت های رسانه های اجتماعی، بسیار مهم است بدانید و درک خطرات احتمالی مربوط به حریم خصوصی چیست؟

خطرات احتمالی در مورد شبکه های اجتماعی

امروزه هکرها شبکه های اجتماعی را به دنبال قربانیان می اندازند. آنها تمایل دارند از URL های کوتاه مانند آنچه که با bit.ly ایجاد می شود استفاده کنند. آنها از این URL های کوتاه استفاده می کنند تا قربانیان خود را برای بازدید از سایت های مضر یا تزریق ویروس به رایانه های خود و یا تلفن های همراه مورد استفاده قرار دهند. هکرها همچنین از نرم افزارهای جاسوسی استفاده می کنند که از طریق دانلود، ایمیل، URL های کوتاه یا پیام های فوری به راحتی بر روی تلفن همراه، لپ تاپ، iPad و یا کامپیوتر شما از راه دور نصب می شوند. نرم افزار جاسوسی اطلاعات هکر را در مورد گذرواژه هایی که در شبکه های اجتماعی و دیگر حساب های شما به صورت آنلاین استفاده می کنید، به شما می دهد. ساده ترین راه برای جلوگیری از قربانی شدن این است که هرگز روی لینک ها کلیک نکنید مگر اینکه مطمئن باشید که از منبع واقعی است.

اکثر شبکه های اجتماعی اطلاعاتی دارند مانند روز تولد و آدرس ایمیل شما. دزد شناسایی تمایل دارند اطلاعات شخصی قربانیان خود را از اطلاعات موجود در شبکه های اجتماعی جمع آوری کنند. بسیاری از دزدان هویت به راحتی با استفاده از اطلاعات شخصی موجود در نمایه شبکه های اجتماعی تمایل دارند حساب های ایمیل قربانیان خود را هک کنند. به عنوان مثال، یکی از رایج ترین تکنیک های استفاده شده توسط دزدان هویت، کلیک کردن بر روی "رمز عبور را فراموش کرده" و سپس در تلاش برای بازیابی رمز عبور از طریق ایمیل. هنگامی که آنها به حساب ایمیل شما دسترسی پیدا می کنند، اساسا به تمام اطلاعات شخصی شما دسترسی دارند.

شبکه های اجتماعی از برنامه های تلفن همراه و خدمات مبتنی بر مکان استفاده می کنند تا کاربران بتوانند در مکان های فعلی خود چک کنند. این به طور معمول مکان فعلی کاربر را به همه افرادی که در شبکه های رسانه ای خاص خود مرتبط هستند، نشان می دهد. اطلاعات مربوط به ارسال شده توسط افراد مخرب به راحتی می توانید برای ردیابی محل سکونت خود استفاده کنید. علاوه بر این، اطلاع دادن به جامعه آنلاین که در آن هستید و یا جایی که می خواهید، می توانید از قربانیان و دزدان به خانه یا کسب و کار خود دعوت کنید. به عنوان مثال، با ارسال مکان فعلی خود و گفتن اینکه شما در تعطیلات طولانی مدت در استرالیا هستید، به شما اجازه می دهیم که سارقان احتمالی و یا دزدان دقیقا بدانند که کجا هستید، و چه مدت از بین می رود. برای مقابله با چنین خطراتی، نباید برنامه های سفر خود و استفاده از خدمات مبتنی بر مکان را نادیده بگیرید..

نکاتی برای محافظت از حریم شخصی شما درشبکه های اجتماعی

رمزهای عبور قوی ایجاد کنید هر چه گذرواژههای قویتری دارند، سخت تر خواهد بود حدس بزنید. شما می توانید کاراکترهای خاصی مانند علامت ها، اعداد و حروف بزرگ را در رمز عبور خود وارد کنید. همچنین از کلمه عبور معمولی مانند نام فرزندتان، نام همسر یا تولد استفاده نکنید.

پروفیل های شبکه های اجتماعی خود را مرور کنید و توجه دقیقی به نحوه هر گونه مشخصات به شما می دهد تا از اطلاعات شخصی حساس محافظت کنید. برخی از شبکه های اجتماعی مانند فیس بوک به شما امکان دسترسی محدود به دوستان، اعضای خانواده و همکاران خود را می دهند. همچنین از گزینه های حفظ حریم خصوصی تقویت شده توسط شبکه های اجتماعی مانند مسدود کردن پیام ها از غریبه ها استفاده کنید. برای اکثر مردم، تنظیمات آنها به طریقی تنظیم می شود که مورد علاقه فیسبوک آنها به راحتی قابل مشاهده برای هر کسی است. استراتژی هایی وجود دارد که می تواند برای جلوگیری از سوء استفاده از افراد در فیس بوک استفاده شود.

آنتی ویروس خوب و ضد جاسوس افزار را نصب کنید؛ ضروری است که یک نرم افزار داشته باشید که از شما محافظت از نرم افزارهای مخرب، ویروس ها و نرم افزارهای جاسوسی را می دهد. دریافت آخرین نرم افزار آنتی ویروس و ضد جاسوس افزار و مطمئن شوید که شما آن را به طور مرتب با تمام آخرین تعاریف بدافزاری به روز رسانی شده است. برای امنیت بیشتر، شما می توانید تمام برنامه های مهم، از جمله سیستم عامل، مرورگرهای اینترنتی خود و دیگر برنامه هایی را که مستعد حملات هستند، به روز کنید.

هنگامی که از شبکه های اجتماعی استفاده می کنید، اساسا اطلاعات شخصی را بصورت آنلاین می گذارید. هنگامی که این اطلاعات آنلاین ارسال می شود، دیگر خصوصی نیست و ممکن است در نهایت سقوط به دست اشتباه باشد. حتی اگر شما بالاترین اقدامات امنیتی را انجام داده باشید، برخی از دوستان، همکاران و شرکتهای که در رسانه های اجتماعی با آنها ارتباط برقرار می کنید می توانند اطلاعات شخصی شما را از بین ببرند. بنابراین، شما باید بسیار مراقب باشید در مورد آنچه شما آنلاین ارسال، دیگر، شما در نهایت به ارائه سارقان ممکن است، stalkers، سایبر گرگ و دزد شناسایی اطلاعات مورد نیاز برای آسیب رساندن

ارائه راهکار

۱. یکی از مهم‌ترین موارد، ارائه اطلاعات لازم در این حوزه به کاربران است که باید در زمان ثبت‌نام آنان در شبکه‌های اجتماعی انجام پذیرد.

۲. محدود ساختن امکان دسترسی افراد به داده و اطلاعات مورد نظر نیز یکی دیگر از روش‌های حفاظتی است که براساس آن تنها تعدادی از افراد بنا به دلایل خاص از مجوز استفاده و دسترسی به برخی از اطلاعات برخوردارند.

۳. از جمله تکنیک‌های حفاظتی مطرح در این حوزه می‌توان به سیستم‌های رمزنگاری اشاره کرد که براساس آن تنها فردی که کلید رمز را در اختیار دارد می‌تواند به اطلاعات دست یابد.

۴. پنهان‌نگاری اطلاعات است که براساس آن می‌تواند اطلاعات مورد نظر را در قالب یک عامل پوشش دهنده و با حفظ دقت و امنیت از جایی به جایی دیگر منتقل و از استفاده غیر مجاز افراد خودداری کرد.

۵. با توجه به خطراتی که ممکن است در صورت آگاهی از اطلاعات شخصی برای افراد ایجاد شود، لازم است تا با دقت کافی، مطالب را برای اشتراک در شبکه‌های اجتماعی انتخاب کنیم و همچنین نسبت به پذیرش افراد غریبه به عنوان «دوست» در شبکه اجتماعی دقت بیشتری به خرج دهیم..

نتیجه‌گیری

انقلاب گوشی های هوشمند با گسترش دستگاه های ارزان و قابل حمل مجهز به سنسورها (به عنوان مثال، GPS و دوربین)، باعث گردیده جمع آوری اطلاعات حساس بسیار آسان تر از گذشته گردد اشتراک گذاری اطلاعات شخصی ریشه در گرایش عمومی افراد یک جامعه دارد که در مورد خود صحبت می کنند، و توسط ارائه دهندگان رسانه های اجتماعی مورد سوء استفاده قرار می گیرد.

همواره این مطلب بر اهمیت حفاظت از اطلاعات شخصی کاربران شبکه اجتماعی تاکید دارد که آگاهی کاربران از خطرات و تهدیدات حریم خصوصی نیاز به توسعه یک سیستم حفظ حریم خصوصی جدید با پشتیبانی از دستگاه های تلفن همراه را برجسته می کند. از آنجا که اکثر کاربران از تلفن های همراه خود برای سرویس های اینترنتی استفاده می کنند،تنظیمات حریم خصوصی که با تلفن های همراه سازگار هستند باید توسعه یابند.از طرفی حریم خصوصی افراد با عملکرد کاربران در فضای مجازی ارتباط مستقیم دارد و با هر کلیکی توسط کاربر احتمال نقض حریم خصوصی توسط افراد فرصت طلب وجود دارد پس کاربران فضای مجازی به عنوان یکی از لایه های امنیت می توانند با ارتقاء دانش سایبری خود و توسعه آن در برقراری امنیت در فضای سایبر قدم های مثبتی بردارند.

منابع

فخار، فاطمه (۱۳۹۵). حفاظت از حریم شخصی در شبکه های اجتماعی. تهران: انتشارات ناقوس.

سلیمی، سعید و محمدنژاد، حسن (تیر، ۱۳۹۵). فضای مجازی و شبکه های اجتماعی. تهران: پشتیبان.

حسین چترودی، مهدیه و اخزمی، مصطفی (۱۳۹۴). بررسی فرصتها و تهدیدهای شبکه های اجتماعی در فضای مجازی، چهارمین همایش سراسری علوم و مهندسی دفاعی در سپاه.

مرجع

ویکی پدیا.

https://fa.wikipedia.org/wiki/%D8%B4%D8%A8%DA%A9%D9%87_%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%DB%8C.پدیا ,

مرکز ماهر. برگرفته از سایت https://www.certcc.ir/news/entry/17, خرداد ۱۳۹۶

سلیمی. سعید و محمدنزاد. فضای مجازی و شبکه های اجتماعی , تیر۱۳۹۵.
فخار. فاطمه. حفاظت از حریم شخصی در شبکه های اجتماعی, ۱۳۹۵.
.
https://www.privacyrights.org
http://scholarcommons.scu.edu/engl_176
http://social-networks-privacy.wikidot.com/
https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html
https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services
https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html.

Privacy in cyberspace

Ali Gorzoddin *[1], Hossein Sadeghi Kashan [2]

Received: 21-01-2019 Revised: 08-06-2019 Accepted: 04-08-2019

Abstract

Social networking has created a huge shift in information sharing and virtual social interactions across the country, with user privacy being a concern for users of service companies as the number of users on social networks grows every day.

In general, the increase in the number of users of social networks has caused security breaches in social networks. Identity theft, surveillance and cyber-bullying are just some of the problems that have arisen that show that privacy is not fully supported by social networks, which is a concern for users of these networks.

Today we can access any information about anyone at any time from anywhere, but this is a new threat to users' private and confidential information. Breaking the privacy of people of all classes and levels can lead to psychological and social insecurity and can have irreparable consequences. The purpose of this study, in addition to identifying the services offered as social networks in cyberspace and categorizing their types, is to investigate the concept of privacy in cyberspace and the challenges for privacy breaches in social networks.

Keywords: Internet, social networks, privacy.

[1]*- ---------- Email:

[2]- Master of Criminal Law and Criminology, Islamic Azad University