امنیت در شبکه‌های اجتماعی

امنیت در شبکه‌های اجتماعی

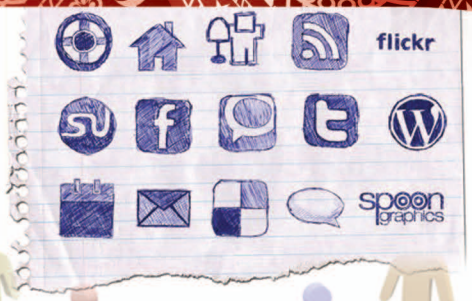
تهیه‌کننده: پلیس فضای تولید و تبادل اطّلاعات ناجا
سال انتشار: ۱۳۹۰
نوبت انتشار: اوّل
پنجمین نمایشگاه بین‌المللی رسانه‌های دیجیتال
با همکاری مرکز توسعه‌ی فنّاوری اطّلاعات و رسانه‌های دیجیتال وزارت فرهنگ و ارشاد اسلامی

مقدّمه

شبکه‌های اجتماعی، گونه‌ای از وب‌سایت‌های اینترنتی هستند که افراد، گروه‌ها و سازمان‌ها، در آن‌ها پیرامون یک یا چند ویژگی مشترک گردهم می‌آیند و اطّلاعات، مطالب و محتواهای خود را با یکدیگر به اشتراک می‌گذارند.

با ظهور و بروز تکنولوژی‌های جدید وب مثل وب ۲.۰ و وب معنایی، شبکه‌های اجتماعی که مبتنی بر تعامل کاربران در ارتباط‌گیری، تولید و به اشتراک‌گذاری محتوا هستند، به وجود آمدند تا جایی که مجموع کاربران معروف‌ترین شبکه‌های اجتماعی اینترنت، به بیشتر از یک میلیارد کاربر رسیده‌است.

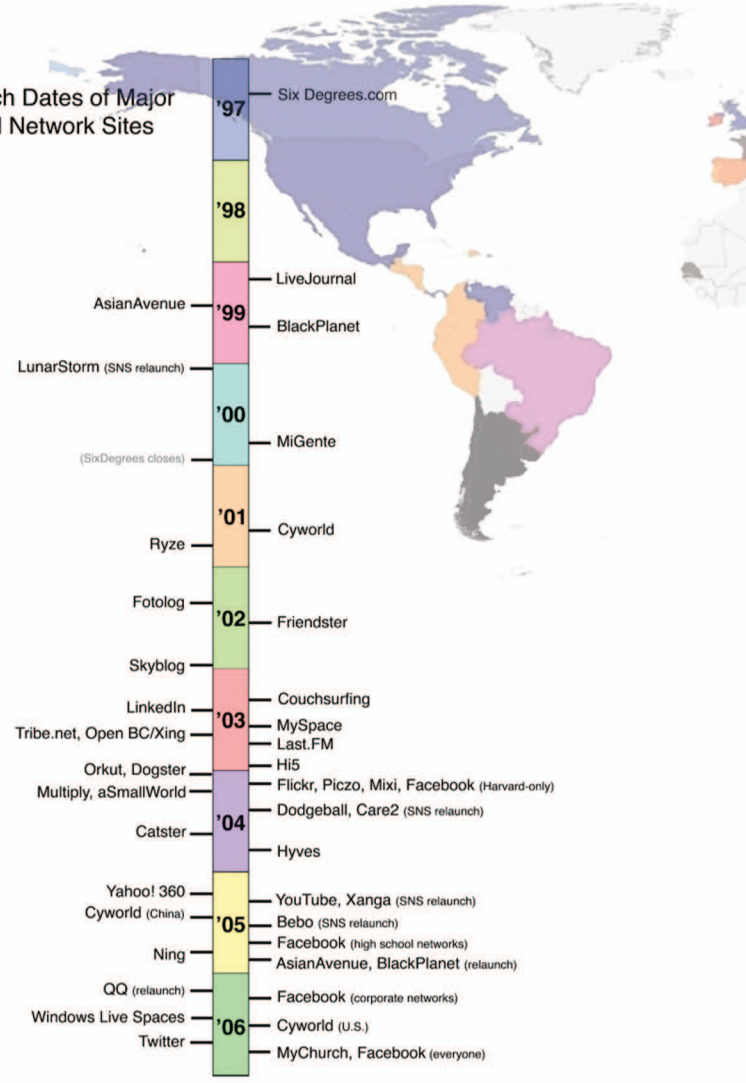
در ماهیّت و پیشینه‌ی شکل‌گیری شبکه‌های اجتماعی اینترنتی، نقل قول‌ها و اظهارنظرهای بسیار متفاوتی وجود دارد. برخی ظهور و بروز این شبکه‌ها را کاملاً طبیعی و در راستای تحوّل موضوع ارتباطات و اطّلاع‌رسانی می‌شمارند امّا بسیاری نیز بر این باورند که در پس پرده‌ی راه‌اندازی این شبکه‌ها، خصوصاً از سوی ایالات متّحده امریکا، منافع اقتصادی، تجاری، سیاسی و امنیتی فراوانی وجود دارد.



شبکه‌های اجتماعی بر پایه‌ی تئوری معروف «شش درجه جدایی» به وجود آمدند و جالب است که این تئوری و بهره‌برداری‌های از آن کاملاً مورد علاقه‌ی سیستم‌های اطّلاعاتی و امنیتی است. ظنّ استفاده از شبکه‌های اجتماعی برای جمع‌آوری اطّلاعات و اشراف اطّلاعاتی و یا حتّی جاسوسی وقتی تقویت می‌شود که مشاهده می‌کنیم پس از واقعه‌ی یازده سپتامبر ۲۰۰۱ در امریکا که نقاط ضعف دستگاه‌ها و لایه‌های امنیتی ایالات متّحده را بیش از پیش آشکار کرد، شبکه‌های اجتماعی اینترنتی از رشد قابل توجّهی برخوردار شدند. به نحوی که معروف‌ترین وب‌سایت‌های شبکه‌های اجتماعی مثل ارکات، لینکداین، مای‌اسپیس، فیس‌بوک و توئیتر که بیشترین کاربران شبکه‌های اجتماعی را در دنیا به خود اختصاص داده‌اند در بعد از این تاریخ به وجود آمده‌اند.

ظاهراً با توجّه به شکست لایه‌های اطّلاعاتی و امنیتی ایالات متّحده در اشراف به القاعده و عدم شناخت قبلی این سرویس‌ها از عاملان حملات انتحاری به ساختمان‌های مرکز تجارت جهانی در نیویورک و ابهامات در چگونگی و کیفیت ارتباط آنان با سران القاعده، این نیازمندی در سیستم‌های اطّلاعاتی و امنیتی به وجود آمد که دامنه‌ی اشراف خود را در دنیا گسترش داده و به آن عمق ببخشند. لذا از شبکه‌های اجتماعی برای اشراف، تحلیل و بررسی رابطه‌ی بین افراد، گروه‌ها، دسته ها و مطالعه‌ی کیفیت و چگونگی رابطه‌های آنان برای مقاصد اطّلاعاتی استفاده می‌کنند.

از سوی دیگر بدیهی است که هزینه‌های سرسام‌آور این وب‌سایت‌ها که خدمات خود را به صورت رایگان عرضه می‌کنند نمی‌تواند تنها از طریق تبلیغات تأمین شود و منطقی است که وب‌سایت های شبکه‌های اجتماعی، مخارج خود را از طریق فروش اطّلاعات تجاری و غیرتجاری که با داده کاوی در انبوهی از اطّلاعات کاربران و محتواهای چندرسانه‌ای آنان به دست آمده‌است تأمین کنند. از این رو محرمانگی اطّلاعات کاربران از سوی این گونه از وب‌سایت، ادّعایی بیش نیست.



کارکردهای شبکه‌های اجتماعی

در هر کشور و هر جامعه‌ای متناسب با فرهنگ، تعاملات اجتماعی و فعّالیّت‌های سیاسی و اقتصادی، کارکردهای شبکه‌های اجتماعی با هم متفاوت است. امّا برخی کارکردهای شبکه‌ای در تمامی جوامع با هم مشترک است.

مهم‌ترین کارکرد شبکه‌های اجتماعی ایجاد گروه‌ها و دسته‌های ارتباطی (Community) پیرامون ویژگی یا ویژگی‌های خاص است. همچنین کارکردهای اقتصادی، مبتنی بر بازاریابی اجتماعی نیز از دیگر کارکردهای این شبکه‌هاست. کارکرد دیگری که برای این شبکه‌ها متصوّر است کارکرد سیاسی است. ایجاد کمپین‌های سیاسی، فعّالیّت‌های دسته‌ها، گروه‌ها و افراد سیاسی در یک فضای اجتماعی اینترنتی از کارکردهای شبکه‌های اجتماعی است.

البته کارکرد سیاسی این شبکه‌ها مورد سوء استفاده‌ی قدرت‌های استکباری قرار گرفته‌است. به نحوی که با طرّاحی اقدامات تبلیغاتی و رسانه‌ای، از وب‌سایت شبکه‌های اجتماعی به عنوان ابزاری برای ایجاد آشوب و بلوا، جنگ روانی و دخالت در امور مختلف کشورهای آزاد استفاده می کنند. اقدامات خصمانه‌ی امریکا و سرویس‌های جاسوسی و اطّلاعاتی سیا و موساد در سال‌های اخیر در فضای شبکه‌های اجتماعی که ایرانی‌ها از آن استفاده می‌کنند، از این دست محسوب می‌شود.

شبکه‌های اجتماعی و حریم خصوصی

حریم خصوصی و محرمانگی اطّلاعات شخصی، یکی از مهم‌ترین و جنجالی‌ترین مباحثی است که از ابتدای همگانی شدن اینترنت و بعدتر با ظهور و بروز شبکه‌های اجتماعی وجود داشته‌است. تقریباً هیچ کسی پیدا نمی‌شود که بخواهد اطّلاعات شخصیِ فردی و خانوادگی خود را به راحتی در اختیار دیگران بگذارد.

در کشورهای غربی، سیاست محرمانگی (Privacy Policy) یکی از ارکان کاربری اینترنت است، به نحوی که قوانین و مقرّرات موضوعه ایجاب می‌کند که در تعامل بین وب سایت‌ها، خدمات‌دهندگان اینترنتی و کاربران، ضمن تعریف سیاست محرمانگی، این امر به نحو مطلوبی در وب‌سایت خدمات‌دهنده به رؤیت کاربر رسیده، حقوق و تکالیف وی یادآوری گردد.

بر اساس سیاست محرمانگی خدمات‌دهندگان و کاربران توافق می‌کنند که چه اطّلاعاتی از آنان به نمایش درآید یا به هر نحو مورد استفاده قرار گیرد. اگر به هر شکل دیگری، خارج از توافق‌نامه‌ی محرمانگی، اطّلاعات کاربران مورد سوءاستفاده قرار گیرد، کاربران امکان اقامه ی دعوی و طرح شکایت را علیه وب‌سایت خدمات‌دهنده خواهند داشت.

معمولاً در شبکه‌های اجتماعی، جزئی‌ترین اطّلاعات کاربران نیز قابل دریافت و انتشار است. علاقمندی‌ها، میزان تحصیلات، ارتباطات خانوادگی، ارتباطات دوستانه، شغل، محلّ زندگی، محل تحصیل و محلّ تولّد و بسیاری از جزئیات دیگر مورد سوال قرار می‌گیرد. برخی از وب سایت‌های شبکه‌های اجتماعی، حتّی رنگ مو، رنگ چشم و اندازه‌ی قدّ کاربر را نیز می‌پرسند.

شبکه‌های اجتماعی و کاربران ایرانی

اگرچه برخی از شبکه‌های اجتماعی خارجی با توجّه به قوانین و مقرّرات جمهوری اسلامی ایران و فعّالیّت‌های مجرمانه‌ای که در فضای آن سایت‌ها صورت می‌گیرد، خارج از دسترسی عادّی قرار دارند، لکن به هر حال بخشی از کاربران ایرانی در این شبکه‌ها عضویت داشته و به انحاء مختلف به آن‌ها دسترسی دارند.

متأسفانه، بررسی‌ها نشان می‌دهد که حضور بسیاری از کاربران ایرانی در فضای شبکه‌های اجتماعی، با مخاطراتی در رابطه با تهدید حریم خصوصی آنان مواجه است و سهل‌انگاری این دسته از کاربران، گاه صدمات و لطمات جدّی بر آنان وارد کرده‌است.

بایستی این حقیقت را پذیرفت که مهم‌ترین چالش شبکه‌های اجتماعی اینترنتی، موضوع «اعتماد» به مخاطب یا کسانی است که در لیست دوستان شما قرار می‌گیرند. مطالعه‌ی سبک کاربری کاربران ایرانی نشان می‌دهد که معمولاً کاربران درخواست سایر کاربران برای دوستی را به راحتی می‌پذیرند. این در حالی است که به طور معمول، در شبکه‌های اجتماعی دوست‌یابی صورت نمی‌پذیرد و تنها دوستان و آشنایان در فضای واقعی در این فضا نیز نسبت به اتّصال و اشتراک گذاری اطّلاعات و محتوا اقدام می‌کنند. در زیر به برخی از نکات مهم در رابطه با تامین امنیت در فضای شبکه‌های اجتماعی اشاره می‌شود.

۱. مراقب جعل هویت باشید: یکی از مهم‌ترین موضوعاتی که کاربران را تهدید می‌کند موضوع جعل هویت است. بخصوص در زمانی که کاربر در زمینه‌ای جزو افراد سرشناس و شناخته‌شده باشد. در صورتی که در حیطه‌ی کسب و کار یا حوزه‌ی اجتماعی خود، فرد سرشناسی هستید، ممکن است افراد دیگری با سوءاستفاده از محتواها و اطّلاعاتی که شما به صورت عمومی به اشتراک گذاشته‌اید، با نام و هویّت جعلی شما و با راه‌اندازی صفحات مشابه دست به اخّاذی، کلاهبرداری و سایر اقدامات مجرمانه بزنند. از این رو هوشیاری در حفظ اطّلاعات و محتواهای خصوصی کاملاً اهمیّت دارد. همچنین در صورتی که متوجّه شدید شخصی با هویّت شما اقدامات مجرمانه صورت می‌دهد، موضوع را به پلیس فتا اعلام کنید.

۲. اسرار ملّی و سازمانی را افشاء نکنید: سازمان، شرکت یا موسّسه‌ای که در آن کار می‌کنید، قطعاً اطّلاعاتی را در اختیار شما می‌گذارد که انتظار دارد شما آن‌ها را به صورت محرمانه نزد خود نگه‌دارید. برخی از شبکه‌های اجتماعی نیز طوری طرّاحی گردیده‌اند که ناخواسته افراد را به ورطه‌ی جاسوسی می‌کشانند. برای مثال برخی شبکه‌های اجتماعی مبتنی بر جانمایی که افراد نام و نشان خیابان‌ها، اماکن و مراکز مهم و حسّاس را به اشتراک می‌گذارند، عملاً کارکرد جاسوسی دارند و به راحتی این امکان را به دشمن می‌دهند که به اطّلاعات مکانی مراکز مهم، حسّاس و حیاتی بدون کمترین زحمتی دسترسی داشته باشد.

۳. مراقب کرم‌های رایانه‌ای و تروجان‌ها باشید: برخی از خدمات شبکه‌های اجتماعی مثل اپلیکیشن‌ها در دل خود، کرم‌های رایانه‌ای و تروجان‌ها را انتشار می‌دهند. بنابر این در فضای شبکه‌های اجتماعی، به هر خدمتی که از سوی کاربران دیگر به شما پیشنهاد می‌شود اعتماد نکنید.

۴. توافق‌نامه‌ی محرمانگی اطّلاعات را مطالعه کنید: با مطالعه‌ی توافق‌نامه‌ی سیاست‌های محرمانگی، متوجّه خواهید شد که کدام دسته از اطّلاعات که شما در شبکه‌های اجتماعی به اشتراک می‌گذارید ممکن است در معرض خطر قرار گیرد. این کار به شما کمک کنید با دقّت بیشتری از این شبکه‌ها استفاده کنید.

۵. به هر ناشناسی اعتماد نکنید: فضای شبکه‌های اجتماعی مملو از کاربرانی است که با هویّت‌های جعلی و برای مقاصد خاص مثل کلاهبرداری، اشاعه‌ی فحشاء و سایر اقدامات غیرقانونی و مجرمانه نسبت به ارتباط‌گیری با کاربران اقدام می‌کنند. از این رو از پذیرفتن افرادی که با هویّت، تصاویر و طرح مطالب اغواکننده سعی در ارتباط‌گیری و افزودن شما به لیست دوستان یا علاقمندان صفحه‌ی خود را دارند، اجتناب کنید.

۶. تنظیمات حریم خصوصی را انجام دهید: تمامی شبکه‌های اجتماعی، ابزارهایی را در اختیار شما می گذارند که نسبت به تنظیم حوزه‌ی حریم خصوصی خود اقدام کنید. با استفاده از این ابزارها می‌توانید با خیال راحت‌تر نسبت به اشتراک‌گذاری اطّلاعات با دوستان اقدام کنید و دسترسی دیگران را محدود نمایید.

امنیت در شبکه‌های اجتماعی

۱۳۹۰