مروری بر امنیت حریم خصوصی در شبکه‌های اجتماعی برخط

کمال‌الدین قضاوتی*[1] و علیرضا نوروزی[2]

[1]مجتمع فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران
kghazavati@yahoo.com

[2]دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران
nowroozi@ce.sharif.edu

چکیده

امروزه شبکه‌های اجتماعی برخط (OSNs) یکی از محبوب‌ترین رسانه‌ها برای ارتباط، اشتراک‌گذاری و انتشار حجم قابل توجهی از اطلاعات است. محبوبیت OSNها اغلب با چالش رفتار با پیام‌های ناخواسته و اهداف مخرب پنهان در آن همراه است. براساس مطالعات اخیر، کاربران شبکه‌های اجتماعی به‌راحتی جزئیات محرمانه و شخصی خود را در معرض دید دیگران قرار می‌دهند. سوء استفاده از این اطلاعات در دنیای مجازی و حقیقی آسیب هایی به همراه می‌تواند داشته باشد. در این مقاله، دسته‌بندی اصلی حملات به امنیت و محرمانگی شبکه‌های اجتماعی برخط در چهار دسته حملات کلاسیک، مدرن، ترکیبی و حملات ویژهٔ کودکان بیان شده است. راه‌های مقابله‌ای که می‌توان برای حفاظت از کاربران OSN در برابر انواع مختلف حملات به‌کار رود، از طرف اپراتورهای شبکه اجتماعی، شرکت‌های امنیتی و پژوهش‌گران ارائه شده است. در انتها نیز هشت راه‌کار پیش‌گیری از این تهدیدها ارائه شده است.

واژگان کلیدی: شبکه‌های اجتماعی برخط، تهدیدهای شبکهٔ اجتماعی، حریم خصوصی، امنیت

۱- مقدمه

در سال‌های اخیر، استفاده از شبکه‌های اجتماعی برخط به‌شدت افزایش یافته به‌طوری‌که این شبکه‌ها در تسهیل ارتباطات روزمره افراد مورد استفاده قرار می‌گیرد. شبکه‌های اجتماعی برخط همچون فیسبوک، گوگل+، Linkedin، Sina Weibo، Twitter، Tumblr، و VKontakte (VK) روزانه صدها میلیون کاربر فعال دارند. برای مثال، فیسبوک ماهانه بیش از ۱,۲۳ میلیارد کاربر فعال دارد، که در این میان ۹۴۵ میلیون از آنها، کاربران موبایلی فیسبوک هستند [۱].

کاربران فیسبوک به‌طورکلی بالای ۱۵۰ میلیارد ارتباط دوستی دارند و به‌طور متوسط بیش از ۳۵۰میلیون عکس در فیسبوک به اشتراک می‌گذارند [۲]. متأسفانه، بیشتر کاربران OSNها از مخاطرات امنیتی که در این نوع از ارتباطات وجود دارد، شامل خطرات محرمانگی [۳، ۶۵، ۶۶، ۶۷]، سرقت هویت، بدافزار و نمایه‌های جعلی (که در برخی موارد اشاره به sybils [۴] یا socialbotها [۵] دارد) ناآگاه هستند. مطالعه‌ای که توسط Dwyer و همکارانش [۶] انجام شده، نشان می‌دهد کاربران فیسبوک و MySpace به این OSNها، و کاربران این شبکه‌های اجتماعی اعتماد دارند. این اعتماد منجر به اشتراک اطلاعات و توسعه روابط جدید می‌شود. علاوه براین، براساس مطالعات اخیر [۷]، بسیاری از کاربران OSN اطلاعات شخصی را به معرض نمایش می‌گذارند و جزئیات درباره خودشان، دوستانشان، و روابطشان، چه با پست‌کردن عکس یا ارائه اطلاعات مستقیم همچون نشانی و شماره تلفن خانه بیان می‌کنند. علاوه براین، بر اساس مطالعات Boshmaf و همکارانش [۳] و Elyashar و همکارانش [۸]، کاربران فیسبوک درخواست‌های دوستی از افراد ناشناس را می‌پذیرند. با پذیرش این درخواست‌های دوستی، کاربران با ناآگاهی، اطلاعات محرمانه‌شان را برای تمام افراد ناشناس فاش می‌کنند.

*نویسندهٔ مسؤول

به محض این‌که استفاده از OSNها در زندگی روزمره کاربران گسترش پیدا کرد، اطلاعات شخصی به‌سادگی در معرض نمایش گذاشته شد و مورد سوء استفاده قرار گرفت. در همین اواخر برداشت اطلاعات، توسط خود اپراتورهای OSN و هم توسط شرکت‌های تجاری واسط، به‌عنوان نگرانی امنیتی قابل توجه برای کاربران OSN شناسایی شده است. شرکت‌ها از اطلاعات شخصی برداشت شده برای اهداف مختلفی می‌توانند استفاده کنند، که تمام آنها می‌تواند محرمانگی کاربر را به خطر اندازد. برای مثال، شرکت‌ها از اطلاعات خصوصی جمع‌آوری‌شده برای متناسب‌کردن تبلیغات برخط براساس نمایه کاربر، به‌منظور دستیابی به ارتباط سودآور در رابطه با مشتریانشان، و یا حتی در اختیار گذاشتن داده‌های شخصی و خصوصی کاربران با دولت مردان [۹] می‌توانند استفاده کنند. این اطلاعات ممکن است، شامل داده‌های عمومی، همچون سن، جنسیت، و درآمد باشد؛ با این وجود، در برخی موارد اطلاعات حساس‌تر و با پتانسیل آسیب‌رسانی بیشتری در معرض دید می‌تواند قرار گرفته باشد. این نگرانی‌های محرمانگی، زمانی بیشتر می‌شود که بدانیم در OSNها: اطلاعات راجع به یک کاربر شبکه حتی بدون دسترسی مستقیم نمایه برخط افراد می‌تواند به‌دست آورده شود؛ جزئیات خصوصی فرد نیز با جمع‌آوری داده‌ها از دوستان کاربر می‌تواند استنتاج شود.

برای مقابله با تهدیدهای یادشده در بالا، چندین راه‌حل توسط اپراتورهای OSN، شرکت‌های امنیتی و پژوهش‌گران دانشگاهی پیشنهاد شده است. OSNها، همچون فیسبوک، برای اطمینان از اینکه کاربر ثبت‌شده یک شخص واقعی است، تلاش می‌کنند از کاربرانشان با اضافه‌کردن فرایندهای تشخیص هویت محافظت کنند [۱۰، ۱۱]. علاوه‌براین، بسیاری از اپراتورهای OSN نیز از پیکربندی تنظیمات محرمانگی کاربر که کاربران را قادر به محافظت از داده‌های شخصی‌شان از دیگر کابران داخل شبکه می‌کند، پشتیبانی می‌کنند [۱۲]. در تنظیمات محرمانگی، اپراتورهای OSN در حال حاضر با کشمکش در علاقه‌مندی[1] روبه‌رو هستند: به این معنی که از یک طرف، از آنجایی که اطلاعات شخصی وسیله مناسبی است، هرچه بیشتر به اشتراک گذاشته شود، بهتر است. از طرف دیگر، کاربری که در رابطه با محرمانگی خود نگران است، اطلاعات کمتری را می‌تواند به اشتراک گذاشته و کمتر فعال باشد. با این وصف، هر دو تنظیمِ مجوزدهی و عمومی‌سازی برای مورد توجه قراردادن محرمانگی تلاش می‌کنند [۱۳]. امروزه سازوکارهای محافظتی اضافی وجود دارد که شامل مقابله با هرزمحتواها [۱۴، ۱۵، ۱۶]، نمایه‌های جعلی [۱۷، ۱۸، ۱۹]، و دیگر تهدیدها است. برای مثال، شرکت‌های امنیتی همچون Websense،Check Point ، و Infoglide ابزارهای اجتماعی برای محافظت کاربران در دنیای OSN پیشنهاد می‌کنند. تهدیدهای جدید بسیار فراگیر هستند تا جایی که جامعه علمی به این موضوع با انتشار پژوهش‌هایی برای حل تهدیدهای مختلف OSN تلاش و راه‌کارهایی برای محافظت از هویت ارائه کرده است [۲۰].

۲- کاربرد شبکهٔ اجتماعی برخط

امروزه بسیاری از OSNها ده‌ها میلیون کاربر ثبت‌شده دارند. فیسبوک، با بیش از یک‌میلیارد کاربر فعال، در حال حاضر بزرگ‌ترین و محبوب‌ترین شبکه اجتماعی دنیا است [۲۱]. دیگر OSNهای شناخته‌شده گوگل+، با بیش از ۲۳۵ میلیون کاربر فعال، توئیتر، با بیش از دویست میلیون کاربر فعال، و LinkedIn، با بیش از ۱۶۰ میلیون کاربر فعال هستند. درحالی‌که برخی کارشناسان اصرار دارند OSNها رسانه‌هایی گذرا هستند و سرانجام با رسانه اینترنتیِ دیگری جایگزین می‌شود؛ آمار کاربران حاضر، نشان‌دهندهٔ پایداریِ شبکه‌های اجتماعی است. پژوهشی که به‌تازگی توسط Pew Research Center's Internet and American Life Project [۲۲] منتشر شده است، نشان می‌دهد که ۷۲٪ افراد بزرگسال آمریکایی از سایت‌های شبکه‌های اجتماعی استفاده می‌کنند؛ این آمار در مقایسه با بررسی انجام‌شده در سال Pew ۲۰۰۵ که در آن تنها ۸٪ افراد بزرگسال آمریکایی برخط از سایت‌های شبکه‌های اجتماعی استفاده می‌کردند، افزایش نگران‌کننده‌ای را نشان می‌دهد. علاوه‌براین، بررسی نشان می‌دهد که ۸۹٪ افراد بزرگسال آمریکایی برخط با سن میان ۱۸ تا ۲۹ از سایت‌های شبکه اجتماعی استفاده می‌کنند؛ درحالی که در ۲۰۰۵ تنها ۹٪ از بررسی شرکت‌کننده‌ها در این گروه سنی از این نوع سایت‌ها استفاده می‌کردند. نتیجه این بررسی‌ها با گزارش منتشرشدهٔ قبلی توسط Nielsen [۲۳] منطبق است؛ که در آن بیان می‌کند، شهروندان

[1] conflict of interest

آمریکایی ۲۲٫۵٪ زمان برخط خود را در OSNها و بلاگ‌ها می‌گذرانند؛ بیش از دو برابر زمانی که در بازی‌های برخط (۹٫۸٪) می‌گذرانند. دیگر فعالیت‌های رایجی که زمان شهروندان آمریکایی صرف آنها می‌شود، شامل رایانامه (۷٫۶٪)، پورتال‌ها (۵٫۴٪)، ویدئو و فیلم‌ها (۴٫۴٪)، جستجوها (۴٫۰٪)، پیام فوری (۳٫۳٪) است. مجموع زمانی که در OSNها صرف می‌شود، به‌ویژه در فیسبوک، بسیار زیاد و در حال افزایش است. کاربران آمریکایی در کل ۵۳٫۵ میلیارد دقیقه را در فیسبوک، ۱۷٫۲ میلیارد دقیقه در یاهو، و ۱۲٫۵ میلیارد دقیقه در گوگل صرف کرده‌اند. دستگاه‌های همراه، یا تلفن‌های همراه، به‌عنوان پلت‌فرم‌های استفاده از اینترنت در حال افزایش هستند. بر اساس گزارش فیسبوک تا پیش از ۲۰۱۶، فیسبوک روزانه ۵۵۶ میلیون کاربر موبایل فعال دارد، که این آمار سالانه ۴۹٪ افزایش پیدا می‌کند. علاوه‌براین، برنامه‌های موبایل فیسبوک و گوگل+ به‌ترتیب دومین و چهارمین برنامه‌های پرکاربرد تلفن‌های هوشمند هستند [۲۴]. باید توجه کرد که کاربرد OSNها روی دستگاه‌های همراه نه‌تنها رابطه نزدیک‌تر با شبکه‌های اجتماعی را ترویج می‌کند، بلکه نگرانی‌های محرمانگی بیشتر، به‌ویژه در موضوع جمع‌آوری داده‌های محلی و فرصت‌های ایجادشده برای تبلیغ کنندگان در شناسایی نوع خاصی از کاربران را می‌تواند به همراه داشته باشد.

در کنار محبوبیت در میان بزرگسالان، OSNها در میان کودکان و نوجوانان نیز بسیار محبوبیت دارند. یک مطالعه جامع [۲۵] انجام‌شده در ۲۵ کشور اروپایی با ۲۵۰۰۰ مشارکت‌کننده آمارهای زیر را ارائه کرد: ۶۰٪ از کودکان ۹ تا ۱۶ ساله‌ای که به اینترنت دسترسی دارند، روزانه (به‌طور متوسط ۸۸ دقیقه استفاده) از آن استفاده می‌کنند و ۵۹٪ از آنهایی که ۹ تا ۱۶ ساله‌اند و از اینترنت استفاده می‌کنند در سایت OSN یک نمایه شخصی دارند (۲۶٪ از ۹ تا ۱۰ ساله‌ها؛ ۴۹٪ از ۱۱ تا ۱۲ ساله‌ها؛ ۷۳٪ از ۱۳ تا ۱۴ ساله‌ها؛ ۸۲٪ از ۱۵ تا ۱۶ ساله‌ها). توجه داشته باشید که قوانین شبکه‌های اجتماعی به‌طوررسمی اجازه استفاده را به افراد زیر ۱۳ سال نمی‌دهد. علاوه‌براین، ۲۶٪ از کودکان در مطالعه همان کشورهای اروپایی نمایه شبکه اجتماعی خود را به‌صورت "public" قرار داده‌اند (به معنای دردسترس برای اشخاص ناشناس)، ۱۴٪ نشانی و شماره تماس را در نمایه خود وارد کرده‌اند، و ۱۶٪ پذیرفته‌اند که در نمایه خود سن غیرواقعی قرار داده‌اند. علاوه‌براین، ۳۰٪ کودکان بررسی‌شده یک تماس برخط با شخصی که هرگز با وی روبه‌رو نشده‌اند، داشته‌اند؛ ۹٪ واقعاً ملاقات رودررو با شخصی داشته‌اند که با وی تنها ارتباط برخط برقرار کرده‌اند؛ ۹٪ تجربه سوء استفاده داده‌های شخصی داشته‌اند؛ ۲۱٪ برخورد با یک یا چند نوع محتوای آسیب‌رسان تولیدشده توسط کاربران را گزارش داده‌اند؛ و ۶٪ دریافت پیام‌های مضر و مخرب در اینترنت را اعلام کرده‌اند. این یافته‌ها ادعاهای قبلی را تصریح می‌کند: استفاده از OSNها در زندگی روزمرهٔ کودکان و نوجوانان وارد شده‌است، و می‌تواند در سوء استفاده از اطلاعات شخصی نمایش گذاشته‌شده، نمایان شود. موضوع قابل توجه این است که، به‌طورتقریبی یک‌سوم والدین مورد مطالعه در کشورهای اروپایی ادعا کرده‌اند که استفاده کودکانشان را از اینترنت فیلتر کرده‌اند، درحالی‌که یک‌چهارم، استفاده از ابزارهای نظارتی را ابراز کرده‌اند.

۳- تهدیدهای شبکه‌های اجتماعی

با افزایش استفاده از OSNها، بسیاری از کاربران از اینکه آشکارا در معرض تهدیدهای امنیتی و محرمانگی هستند، آگاهی ندارند. این تهدیدها به چهار دسته اصلی می‌تواند تقسیم‌بندی شود. دسته نخست شامل تهدیدهای کلاسیک است، یعنی تهدیدهای امنیتی و محرمانگی که نه‌تنها کاربران شبکه اجتماعی را به خطر می‌اندازد، بلکه کاربران اینترنت را که از شبکه‌های اجتماعی استفاده نمی‌کنند، نیز تهدید می‌کند. دسته دوم تهدیدهای مدرن است، تهدیدهایی که مختص شبکه‌های اجتماعی هستند و در آن استفاده از بستر OSN برای امنیت و محرمانگی کاربر خطرآفرین است. دسته سوم شامل تهدیدهای ترکیبی است؛ که در آنجا شرح داده شده است که چگونه مهاجم حملات مختلفی را به‌منظور ایجاد حملات مهلک و پیچیده می‌تواند ترکیب کند. چهارمین و آخرین دسته‌بندی شامل تهدیدهایی است که کودکان استفاده‌کننده از شبکه‌های اجتماعی را تهدید می‌کند. در ادامه این تهدیدها را به‌صورت مشروح بیان می‌کنیم.

۱ -۳- تهدیدهای کلاسیک

تهدیدهای کلاسیک مسئله‌ای است که همواره از زمان گسترش کاربرد اینترنت وجود داشته است که اغلب به مواردی همچون بدافزار، هرزمحتوا، حملات cross-site

scripting (XSS)، یا فیشینگ اشاره دارد. هرچند این حملات از گذشته وجود داشته‌اند، اما پیوسته ساختار و نهاد OSNها را هدف قرار داده‌اند و به سرعت میان کاربران شبکه می‌تواند گسترش پیدا کند. تهدیدهای کلاسیک از مزیت انتشار اطلاعات شخصی در شبکه اجتماعی برای پیاده‌سازی حمله نه‌تنها برای کاربر، بلکه برای دوستان کاربر که به اطلاعات شخصی وی دسترسی دارند نیز می‌تواند به‌کار گرفته شود.

برای مثال، یک مهاجم می‌تواند کد مخربی را درون پیام هرزمحتوای جذابی که از جزئیات اطلاعات نمایه کاربر فیسبوک بهره گرفته است، قرار دهد. به‌دلیل مهارت در به‌کارگیری اطلاعات شخصی در این پیام، احتمال اینکه کاربر پیام را باز کند و به سبب آن آلوده شود، وجود دارد. در بسیاری موارد، این تهدیدها اطلاعات ضروری و روزمرهٔ افراد همچون شماره کارت اعتباری، رمز عبور حساب کاربری، توان محاسباتی سامانه، و حتی پهنای باند (به‌منظور ارسال رایانامه‌های هرزنامه) را هدف قرار می‌دهد. همچنین این نوع از تهدیدها از کاربر آلوده‌شده با دزدیدن نشست به‌منظور پست‌کردن پیام و یا حتی تغییر اطلاعات شخصی کاربر می‌تواند سوء استفاده کند.

تهدیدهای کلاسیک مختلف در ادامه توضیح داده شده‌اند، که در سناریوهای واقعی برای محرمانگی و امنیت کاربر می‌توانند خطر آفرین باشند.

بدافزار: بدافزار نرم‌افزار مخربی است که با هدف مختل‌کردن عملکرد رایانه به‌منظور جمع‌آوری اعتبارنامه‌های کاربر و گرفتن دسترسی از اطلاعات خصوصی توسعه داده می‌شود. بدافزارها در شبکه‌های اجتماعی از ساختار OSN برای انتشار خود میان کاربران و دوستانشان در شبکه استفاده می‌کنند. در برخی موارد، بدافزار می‌تواند از اعتبارنامه به‌دست‌آمده برای جعل هویت کاربر و ارسال پیام‌هایی به دوستان برخط کاربر به‌جای کاربر واقعی اقدام کند. Koobface نخستین بدافزاری بود که با موفقیت از طریق OSNها همچون فیسبوک، MySopce، و توئیتر منتشر شد. به‌محض آلوده‌سازی، Koobface تلاش خود را برای جمع‌آوری اطلاعات ورود به سیستم قربانی و اتصال رایانه آلوده به بخشی از یک شبکه بات، تشکیل رایانه‌هایی با نام "ارتش زامبی‌ها" برای انجام فعالیت‌های مجرمانه، همچون ارسال پیام‌های هرزمحتوا و حمله به دیگر رایانه‌ها و سرورها را در اینترنت آغاز می‌کرد.

حملات فیشینگ: حملات فیشینگ یک شکل از مهندسی اجتماعی برای به‌دست‌آوردن اطلاعات حساس و خصوصی با جعل هویت به‌عنوان یک واسط مورد اعتماد است. مطالعهٔ اخیر [۲۶] نشان داده است، کاربرانی که با سایت‌های شبکه‌های اجتماعی تعامل می‌کنند، بیشتر در معرض افتادن در دام کلاه‌برداری‌های فیشینگ به‌دلیل ذات اجتماعی و اعتماد در این شبکه‌ها هستند. علاوه براین، در سال‌های اخیر، تلاش‌های انجام‌شده برای حملهٔ فیشینگ در شبکه‌های اجتماعی به‌سرعت در حال افزایش است. براساس گزارش آژانس امنیتی مایکروسافت [۲۷]، ۸۴٫۵٪ از تمام حملاتِ فیشینگ، کاربران شبکه‌های اجتماعی را هدف قرار داده است. نوعی از حملات اتفاق‌افتادهٔ فیشینگ در فیسبوک، کاربران را به صفحه جعلی ورودی فیسبوک هدایت می‌کرد؛ سپس، حمله فیشینگ میان کاربران فیسبوک از طریق دعوت از دوستان برای فشردن روی پیوند ارسال‌شده در فضای نمایه کاربر اصلی انجام می‌شد [۲۸].

تولیدکنندگان هرزمحتوا: تولیدکنندگان هرزمحتوا کاربرانی هستند که از سامانه‌های پیام الکترونیکی به‌منظور ارسال پیام‌های ناخواسته، همچون تبلیغات، به دیگر کاربران استفاده می‌کنند. تولیدکنندگان هرزمحتوای OSN از بستر شبکهٔ اجتماعی برای ارسال پیام تبلیغاتی به دیگر کاربران با ایجاد نمایه‌های جعلی اقدام می‌کنند. تولیدکنندهٔ هرزمحتوا همچنین از بستر OSN برای اضافه‌کردن پیام‌های نظرات به صفحاتی که توسط بسیاری از کاربران شبکه دیده می‌شود، می‌تواند استفاده کند. یک مثال از شیوع هرزمحتوای اجتماعی را در توئیتر می‌توان ذکر کرد، که متحمل حجم زیادی از هرزمحتواها شده بود. در آگوست ۲۰۰۹، ۱۱٪ از پیام‌های توئیتر پیام‌های هرزمحتوا بودند. با این وجود، با شروع ۲۰۱۰، توئیتر با موفقیت، درصد پیام‌های هرزمحتوا را به ۱٪ کاهش داد [۲۹]. پژوهش [۳۰] بیان می‌کند، "هرزمحتوای اجتماعی، به‌شکلی که در توئیتر وجود دارد، به رشد خود ادامه خواهد داد؛ مگر اینکه به‌سرعت شناسایی و جلوگیری شود."

Cross-Site Scripting (XSS): حمله XSS یک حمله در برابر برنامه‌های کاربردی وب است. حمله‌کننده‌ای که از XSS استفاده می‌کند، از اعتماد سرویس گیرنده وب در برنامه کاربردی وب سوء استفاده می‌کند و سبب می‌شود، سرویس گیرنده وب کد مخربی را اجرا کند که قادر است، اطلاعات حساس را جمع‌آوری کند. OSNها، که یک نوع از برنامه‌های

کاربردی می‌باشند، می‌تواند متحمل حملات XSS باشند. علاوه براین، مهاجمان از آسیب‌پذیری XSS ترکیب‌شده با زیرساخت OSN برای ایجاد کرم XSS که می‌تواند به‌صورت ویروسی میان کاربران شبکه اجتماعی منتشر شود، می‌توانند استفاده کنند [۳۱]. در آپریل ۲۰۰۹، یک کرم XSS، که Mikeyy می‌نامیدند، به‌سرعت توئیت‌هایی را میان توئیتر ارسال می‌کرد و کاربران بسیاری از این طریق آلوده کرد. کرم Mikeyy از ضعف XSS و ساختار شبکه توئیتر برای انتشار از طریق نمایهٔ کاربران توئیتر استفاده می‌کرد [۳۲].

کلاه‌برداری اینترنتی: کلاه‌برداری اینترنتی، که با عنوان کلاه‌برداری سایبری نیز شناخته می‌شود، به به‌کارگیری اینترنت برای کلاه‌برداری یا گرفتن منافع افراد اشاره می‌کند. در گذشته، کلاه‌برداران از شبکه اجتماعی شخصی-سنتی استفاده می‌کردند، مانند ملاقات‌های گروهی هفتگی، تا از این روش بتوانند به‌تدریج یک ارتباط قوی با قربانیان را پایه‌ریزی کنند. در حال حاضر، براساس North American Securities Administrators Association (NASAA) [۳۳]، با افزایش محبوبیت شبکه‌های برخط، کلاه‌برداران برای سوء استفاده از قربانیانشان به سمت OSNها گرایش پیدا کردند؛ به‌گونه‌ای که از اطلاعات شخصی منتشرشدهٔ افراد در نمایه برای رسیدن به هدف خود استفاده می‌کنند.

۲-۳- تهدیدهای مدرن

تهدیدهای مدرن نوعاً مختص محیط OSN است. این تهدیدها به‌طورمعمول اطلاعات افراد و همین‌طور اطلاعات شخصی دوستان فرد مورد نظر را هدف قرار می‌دهند. برای مثال، مهاجمی‌که سعی در دسترسی به نام مدرسه یک کاربر در فیسبوک را دارد -که تنها برای دوستان فیسبوکی فرد قابل مشاهده است- یک حساب جعلی با جزئیات مناسب می‌تواند ایجاد و یک درخواست دوستی به کاربر هدف ارسال کند. اگر کاربر درخواست دوستی را قبول کند، جزئیات اطلاعات برای مهاجم قابل مشاهده خواهد شد. علاوه‌براین، مهاجم داده‌های دوستان فیسبوکی کاربر را می‌تواند جمع‌آوری کرده و یک حمله استنتاجی را برای پی‌بردن به نام مدرسه قربانی از داده‌های جمع‌آوری‌شدهٔ دوستان کاربر پیاده‌سازی کند.

کلیک‌دزدی: کلیک‌دزدی روش مخربی است که در آن کاربران برای کلیک‌کردن روی محتوایی که متفاوت از آنچه تمایل به کلیک آن دارند، فریب می‌خورند. با استفاده از کلیک‌دزدی، مهاجم می‌تواند کاربر را در پست‌کردن پیام‌های هرزمحتوا روی تایم‌لاین فیسبوکی، دادن "like" به پیوندهای ناشناس (که با عنوان لایک‌دزدی هم شناخته می‌شود)، و حتی بازکردن میکروفون و دوربین وب برای ضبط تصاویر فریب دهد.

حملات De-Anonymization: در بسیاری از OSNها همچون توئیتر و MySpace، کاربران محرمانگی و گمنامی خود را با استفاده از نام‌های مستعار می‌توانند حفظ کنند. این حملات از روش‌هایی همچون ردگیری کوکی‌ها، توپولوژی شبکه، و اعضای گروه کاربر برای کشف هویت واقعی کاربر استفاده می‌کند. مثالی از De-Anonymization در [۳۴] شرح داده شد، که ثابت کرد برای یک شخص ثالث این امکان وجود دارد که هویت یک کاربر را با استفاده از اطلاعات مرتبط نشت‌شده در سایر سایت‌های شبکه اجتماعی به‌دست آورد. آنها همچنین نشان دادند که بیش‌تر کاربران مطالعه‌شده در OSNها در برابر نشت اطلاعات هویتی OSN از طریق سازوکارهای ردگیری همچون ردگیری کوکی‌ها آسیب‌پذیر هستند.

تشخیص چهره: بسیاری از افراد از OSNها برای به‌اشتراک‌گذاری تصاویر خود و دوستانشان استفاده می‌کنند. میلیون‌ها میلیون عکس هر روزه در فیسبوک به اشترک گذاشته می‌شود. علاوه‌براین، تصاویر نمایهٔ بسیاری از کاربران فیسبوک برای دیدن و بارگیری عمومی در دسترس هستند. برای نمونه، چهره‌های ثبت‌شده در وب‌سایت فیسبوک به کاربران اینترنتی دیدن تصاویر نمایه حدود ۱,۲ میلیارد کاربر فیسبوک را می‌دهد. این تصاویر برای ایجاد یک پایگاه داده بیومتریک در تشخیص کاربران OSN بدون اطلاع خودشان می‌تواند استفاده شود.

نمایه‌های جعلی: نمایه‌های جعلی (که به sybils و socialbot نیز اشاره می‌کند) نمایه‌های خودکار یا نیمه‌خودکاری هستند که رفتارهای انسانی را در OSNها تقلید می‌کنند. در بسیاری موارد، نمایه‌های جعلی برای جمع‌آوری داده‌های شخصی کاربران از شبکه‌های اجتماعی می‌تواند به‌کار گرفته شود. با ارسال درخواست‌های دوستی به دیگر کاربران در OSN، و تأیید توسط کسانی که اغلب این‌گونه درخواست‌ها را می‌پذیرند، socialbotها داده‌های خصوصی کاربر را که تنها برای دوستان قابل نمایش شده است، می‌توانند جمع‌آوری کنند. علاوه براین، نمایه‌های جعلی برای زمینه‌سازی حملاتSybil، انتشار پیام‌های

هرزمحتوا، یا حتی تغییر آمارهایOSN، می‌توانند به‌کار گرفته شوند. مقاله‌ای درهمین‌اواخر ادعا کرد که بازار خرید دنبال‌کننده‌های جعلی و retweetها جعلی هم‌اکنون یک تجارت چندمیلیون‌دلاری [۳۵] است.

حملات Identity Clone: با استفاده از این روش، مهاجمان نسخه المثنی یک کاربر برخط در همان شبکه، و یا در شبکه‌های مختلف دیگر را برای فریب‌دادن دوستان کاربر اصلی در نظر می‌گیرند، تا بتواند یک رابطه مورد اعتماد با نمایه المثنی ایجاد کند. مهاجم از این اعتماد برای جمع‌آوری اطلاعات شخصی درباره دوستان کاربر یا انجام انواع دیگری از کلاه‌برداری‌های برخط می‌تواند استفاده کند.

حملات استنتاجی: حملات استنتاجی در OSNها برای پیش‌بینی هویت کاربر، اطلاعات حساسی که کاربر آنها را فاش نکرده است، گرایش‌های مذهبی یا گرایش‌های جنسی استفاده می‌شود. این نوع از حملات با استفاده از روش‌های داده‌کاوی ترکیب‌شده با داده‌های عمومیِ دردسترس OSN، همچون توپولوژی شبکه و داده‌های دوستان کاربر می‌تواند پیاده‌سازی شود.

نشت اطلاعات: OSNها این اجازه را به کاربران می‌دهند که به‌صورت آزاد اطلاعات را با دوستان و دیگر کاربران در شبکه به اشتراک گذاشته و معاوضه کنند. در برخی موارد کاربران OSN مایل‌اند اطلاعات حساس همچون اطلاعات مربوط به سلامتی و وضعیت هوشیاری درباره خود و دیگر افراد را به اشتراک گذارند. در مطالعهٔ اخیر، Torabi و Beznosov[۳۶] مشاهده شد که ۹۵٫۸٪ از ۱۶۶ شرکت‌کننده برخی اطلاعات مربوط به سلامتی را از طریق حساب‌های OSN خود به اشتراک گذاشته‌اند. نشت اطلاعات حساس و شخصی ممکن است، برای کاربران شبکهٔ اجتماعی عواقب ناخوشایندی به همراه داشته باشد. برای مثال، کمپانی‌های بیمه‌ای ممکن است از داده‌های OSN برای تشخیص مشتریان پرخطر استفاده کنند. این کمپانی‌ها از نشت اطلاعات OSN برای تشخیص مشتریان با شرایط پزشکی خاص، برای افزایش حق بیمه و یا عدم پوشش دوباره فرد می‌توانند استفاده کنند؛ علاوه براین، کارفرماها از شبکه‌های اجتماعی برای دیدن متقاضیان کار استفاده می‌کنند. بنابراین، نشت اطلاعات شخصی، حتی بیان‌کردن سلایق خصوصی، در OSNها ممکن است، انتخاب‌های آینده برای یافتن کار را به خطر اندازد.

نشت مکانی: با افزایش استفاده از تلفن‌های هوشمند که کاربران را برای به‌اشتراک‌گذاشتن اطلاعات مکانی ترغیب می‌کند، بسیاری از افراد در OSNها تمایل به اشتراک اطلاعات شخصی و در برخی موارد حساس درباره محل تقریبی حال و آینده خود (و دوستانشان) دارند. در مطالعه‌ای که توسط Humphreys و همکارانش [۳۷] انجام گرفته ۲۰٪ توئیت‌های توئیتر آزمایش‌شده شامل اطلاعاتی دربارهٔ زمانی است که افراد به فعالیت‌های مشخصی مشغول شده‌اند، و ۱۲٪ از توئیت‌ها مکان کاربر را بیان کرده‌اند؛ علاوه براین، مطالعه‌ای توسط Mao و همکارانش شرح می‌دهد که دسته‌بندی‌ها در تشخیص‌دادن مکان کاربر توئیتر در زمان واقعی می‌تواند کمک‌کننده باشد. همچنین، Cheng و همکارانش [۳۸] بستری برای تخمین مکان شهری کاربر براساس محتوای توئیت کاربر ارائه کردند. این نوع از اطلاعات در کلاه‌برداری‌ها و اعمال مجرمانه می‌تواند به‌کار گرفته شود.

در برخی موارد، کاربران OSN ناآگاهانه مکان خود را با اشترک‌گذاری بخش‌های رسانه‌ای همچون عکس‌ها و ویدئوها به اشتراک می‌گذارند، که ممکن است، حاوی اطلاعات جغرافیایی ضمیمه‌شده دربارهٔ مکان فعلی و گذشته آنها باشد [۳۹].

Socware: Socware شامل پست‌ها و پیام‌های جعلی و با احتمال آسیب‌رسانی از دوستان در OSNها است. Socware ممکن است، قربانیان را با پیشنهاد پاداش‌های دروغین از طریق نصب برنامه‌های فیسبوکی مخرب مرتبط با socware یا بازدید از وب‌سایت‌های مشکوک socware فریب دهد. پس از آنکه کاربران وب‌سایت socware را بازدید یا برنامهٔ مربوطه را نصب کردند، socware نصب‌شده پیام‌هایی را از طرف کاربر به دوستان کاربر ارسال که در اصل در انتشار ویروسی socware همکاری می‌کند. در ۲۰۱۲، Rahman و همکارانش [۴۰] نزدیک به چهل‌میلیون پست را بررسی و کشف کردند که ۴۹٪ کاربران مطالعه‌شده دست‌کم یکبار در طی چهار ماه با یک socware روبه‌رو شده‌اند. علاوه براین، Rahman و همکارانش [۴۱] پی بردند که ۱۳٪ از ۱۱۱۰۰۰ برنامه‌های بررسی‌شده برنامه‌های مخربی بودند که می‌توانستند در انتشار socware دخالت داشته باشند. همچنین، در مطالعهٔ اخیر توسط Huang و همکارانش [۴۲] اکوسیستمی‌که socwareها را قادر به انتشار می‌کند، مورد بررسی قرار گرفت. با تحلیل داده‌هایی از صفحه نمایه قریب به ۳ میلیون کاربر فیسبوک در طی پنج ماه، آنها کشف کردند که "انتشار

socware توسط برنامه‌های فیسبوکی پشتیبانی می‌شود که در گروه‌های وسیعی با یکدیگر همکاری می‌کنند".

۳-۳- تهدیدهای ترکیبی

امروزه مهاجمان می‌توانند تهدیدهای مدرن و کلاسیک را به‌منظور ایجاد یک حمله پیچیده‌تر ترکیب کنند. برای مثال به این دو سناریو توجه کنید:

سناریوی یک: مهاجم از حمله فیشینگ برای گردآوری رمزعبور کاربر مورد نظر در فیسبوک می‌تواند استفاده کند و سپس پیامی حاوی حمله کلیک‌دزدی روی تایم‌لاین کاربر مورد نظر پست کند؛ سپس دوستان فیسبوکی کاربر را برای کلیک روی پیام پست‌شده و نصب یک ویروس روی رایانه فریب دهد.

سناریوی دو: نمونه دیگر استفاده از نمایه‌های المثنی برای جمع‌آوری اطلاعات شخصی درباره دوستان کاربر کپی‌شده است. با استفاده از اطلاعات شخصی دوستان، مهاجم می‌تواند، پیام‌های رایانه متناسب با اطلاعات به‌دست‌آمدهٔ حاوی یک ویروس ارسال کند. با استفاده از اطلاعات شخصی، ویروس با احتمال بیشتری فعال خواهد شد.

گفتنی است که فرایندهای بازیابی از تهدیدهای مدرن و کلاسیک از یکدیگر متمایزند. به‌منظور بازیابی[1] یک حمله کلاسیک، همچون ویروس، به‌طورمعمول با نصب مجدد سیستم عامل، تغییر گذرواژه یا سوزاندن کارت اعتباری از حمله جلوگیری کرد. با این حال، به‌منظور بازیابی یک حمله OSN مدرن که "هویت شما را به سرقت می‌برد"، تلاش بیشتری باید انجام شود؛ برای اینکه بازنشاندن اطلاعات شخصی بیش از اندازه زمان‌بر است و همواره ممکن نیست. برای نمونه، شما می‌توانید نشانی رایانامه خود را تغییر دهید، اما تغییر نشانی خانه مشکل‌تر است.

۴-۳- تهدیدهایی که کودکان را هدف قرار داده است

کودکان و نوجوانان، مطمئناً تهدیدهای مدرن و کلاسیک را که در بالا ذکر شد، تجربه می‌کنند؛ اما تهدیدهایی وجود دارد که به‌عمد و به‌خصوص کاربران جوان OSNها را هدف قرار می‌دهد.

شکارچیان برخط: نگرانی بزرگ راجع به ایمنی اطلاعاتِ شخصیِ کودکان در برابر کودک‌آزاری اینترنتی است، که به کودک آزاری برخط مشهور است. Livingstone و Haddon [۴۳] از EU Kids Online یک تایپولوژی به‌منظور فهم خطرات و آسیب‌های مرتبط با چنین فعالیت‌های برخطی را تعریف کرده‌اند: آسیب‌های محتوایی (کودک در معرض محتوای غیراخلاقی یا آسیب‌رسان قرار دارد)، آسیب‌های تماسی (کودکی که با یک فرد بزرگسال یا کودک دیگری برای اهداف سوء تماس دارد)، و آسیب‌های رفتاری (کودکی که در آغاز سوء استفاده یا مخاطرات رفتاری است). رفتارهایی که برای بهره‌برداری غیراخلاقی اینترنتی از کودکان در نظر گرفته می‌شود، شامل بزرگسالانی است که از کودکان برای تولید و توزیع ویدئوی غیراخلاقی کودک و توزیع، و استفاده از اینترنت به‌منظور پایه‌ریزی برخط و آفلاین بهره‌برداری غیراخلاقی استفاده می‌کنند. در مطالعه سال ۲۰۰۸، Wolak و همکارانش [۴۴] شکارچیان برخط واقعی و غیرواقعی را آزمایش کردند. Wolak و همکارانش، بیان کردند، بیشتر جرایم اینترنتی با پی‌ریزی یک رابطه میان یک بزرگسال و کودک از طریق یک پیام، رایانامه، چت آغاز می‌شود. با این حال، در بیشتر موارد کودکان از این واقعیت که با یک فرد بزرگسال صحبت می‌کنند، آگاه هستند. برخلاف نظریه رایج، Wolak و همکارانش کشف کردند که بیشتر قربانیان جرایم غیراخلاقی اینترنتی دختران نوجوان (۱۳ تا ۱۷ ساله) هستند، و هیچ گزارشی از زیر ۱۲ سال داده نشده است.

رفتارهای پرخطر: عامل رفتارهای پرخطر کودکان ممکن است، شامل ارتباط برخط مستقیم با افراد ناشناس، استفاده از اتاق‌های چت برای تعاملات با افراد ناشناس، و دادن پیام و عکس خصوصی با افراد ناشناس باشد. باید توجه داشت که هر کدام از رفتارهای ذکرشده در بالا به تنهایی خطرآفرین است و ترکیبی از این رفتارها می‌تواند به شکل قابل توجهی سبب آسیب‌هایی به ایمنی کودک شود. Wolak و همکارانش روشی ارائه کردند که بر اساس آن رفتارهای برخطِ پرخطر و افراد خاصی را که بیشتر در معرض آنها هستند، می‌توان شناسایی کرد.

مزاحمت سایبری: مزاحمت سایبری (که با عنوان سوءاستفاده سایبری نیز نام برده می‌شود) مزاحمتی است که در بستر ارتباطات فناوری همچون رایانامه، چت، گفتگوی

[1] recovery

تلفنی، و OSNها اتفاق می‌افتد، توسط مهاجمی که از این بسترها برای آزار قربانیان با ارسال پیام‌های تکراری آسیب‌رسان، اظهارات غیراخلاقی، یا تهدیدها، با انتشار تصاویر یا ویدیوهای شرم‌آور از قربانیان یا با به‌کارگیری رفتارهای نامناسب دیگر استفاده می‌کند. امروزه، مزاحمت سایبری پدیده رایجی در OSNها شده است که در آن مهاجم از زیرساخت شبکه برای انتشار بی‌رحمانه شایعات درباره قربانیان و اشتراک تصاویر شرم‌آور با دوستان شبکه‌ای قربانی می‌تواند استفاده کند. مزاحمت سایبری به‌طورمعمول کودکان را در مقایسه با بزرگسالان تحت تأثیر قرار می‌دهد. درهمین‌اواخر در یک بررسی برخط، که شامل ۱۸۶۸۷ والدین از ۲۴ کشور است، نشان داده شده که ۱۲٪ والدین ادعا کرده‌اند کودکانشان مورد مزاحمت سایبری قرار گرفته‌اند [۴۵]. علاوه‌براین، بر اساس نتایج، بیش‌تر کودکان این آزار و اذیت را در استفاده گسترده از سایت‌های شبکه‌های اجتماعی همچون فیسبوک تجربه کرده‌اند.

۴- راه‌کارهای مقابله با تهدیدهای شبکه‌های اجتماعی

در سال‌های اخیر، اپراتورهای شبکهٔ اجتماعی، شرکت‌های امنیتی و پژوهش‌گران سعی در مقابله با تهدیدهای یادشده با ارائه راه‌کارهای مختلف داشته‌اند. در این بخش راه‌کارهایی که در محافظت امنیتی و محرمانگی کاربران OSN می‌تواند کمک‌کننده باشد، شرح داده شده است.

۴-۱- اپراتورهای شبکهٔ اجتماعی

اپراتورهای شبکهٔ اجتماعی تلاش می‌کنند با فعال‌کردن معیارهای ایمنی همچون به‌کارگیری سازوکارهای احراز هویت و به‌کارگیری تنظیمات محرمانگی از کاربران خود محافظت کنند. جزئیات چند نمونه از این روش‌ها در ادامه شرح داده شده است.

سازوکارهای احراز هویت: به‌منظور اطمینان از اینکه کاربرِ ثبت نام کرده یا وارد شده به شبکه اجتماعی یک شخص واقعی است و یک socialbot یا یک حساب کاربری تسخیرشده نیست، اپراتورهای OSN از سازوکارهای احراز هویت همچون CAPTCHA، تشخیص عکس دوستان، احراز هویت چندعامله استفاده می‌کنند، و حتی در برخی موارد درخواست می‌شود که کاربر یک رونوشت از شناسه دولتی خود را ارسال کند. برای مثال، سازوکار احراز هویت دو مرحله‌ای که توئیتر اخیراً معرفی کرد، مستلزم این است که کاربر علاوه‌بر ورود رمز عبور در زمان ورود به توئیتر، یک کد تأیید را که به دستگاه موبایل کاربر ارسال می‌شود، نیز وارد کند.

این سازوکار از ورود کاربر مخرب از طریق حساب ربوده شده و انتشار اطلاعات غلط از طریق آن حساب ربوده‌شده جلوگیری می‌کند. چنین سازوکاری خطرات احتمالی را خنثی می‌کند.

تنظیمات امنیت و محرمانگی: بسیاری از OSNها از پیکربندی مختلف تنظیمات محرمانگی که کاربر را قادر به حفاظت از داده‌های شخصی از دیگر کاربران یا برنامه‌های کاربردی می‌کند، پشتیبانی می‌کنند. برای مثال کاربران فیسبوک تنظیمات محرمانگی خود را می‌توانند شخصی‌سازی و انتخاب کنند که کدام کاربر در شبکه (همچون دوستان، دوستانِ دوستان، و هر شخصی) مجاز به دیدن جزئیاتشان، تصاویر، پست‌ها و دیگر اطلاعات شخصی هستند. مثال مشابه از تنظیمات محرمانگی شخصی‌سازی‌شده در گوگل+ است که در آن کاربران هر کدام از دوستانشان را در گروه‌هایی قرار می‌دهند که "حوزه" نامیده می‌شود؛ مانند حوزهٔ بهترین دوستان، حوزهٔ کاری، و حوزهٔ دوستان مدرسه. با استفاده از این حوزه‌ها، کاربران گوگل+ محافظت بهتری از محرمانگی با انتخاب این که کدام پست به کدام حوزه تعلق دارد، می‌توانند داشته باشند. علاوه براین، فیسبوک و گوگل+ به کاربرانشان امکان تأیید یا رد دسترسی برنامه‌های کاربردی را به داده‌های شخصی می‌دهد.

برخی OSNها نیز از پیکربندی‌های امنیتیِ اضافی پشتیبانی می‌کنند که کاربر را قادر به فعال‌کردن مرور امن، دریافت هشدارهای ورود، و فراهم‌کردن دیگر ویژگی‌های امنیتی می‌کند. با این حال، بسیاری از کاربران OSN هنوز از تنظیمات محرمانگی پیش‌فرض استفاده می‌کنند که اجازه نمایش اطلاعاتشان را به افراد ناشناس می‌دهد.

سازوکارهای حفاظتی داخلی: OSNهای مختلف از کاربران خود با پیاده‌سازی سازوکارهای حفاظتیِ داخلیِ اضافی برای دفاع در برابر تولیدکنندگان هرزمحتوا، نمایه‌های جعلی، کلاه‌برداری‌ها، و دیگر تهدیدها محافظت می‌کنند. برای مثال فیسبوک، کاربرانش را از حملات مخرب و جمع‌آوری اطلاعات با فعال‌کردن سامانهٔ ایمنی فیسبوک (FIS) محافظت می‌کند. FIS به‌عنوان یک سامانهٔ یادگیری

شناخته می‌شود که بررسی‌ها و دسته‌بندی‌های برخط لحظه‌ای روی عمل‌های خواندن و نوشتن روی پایگاه داده فیسبوک انجام می‌دهد [۴۶].

گزارش کاربران: اپراتورهای OSN تلاش‌هایی برای محافظت کاربران کودک و نوجوان از آسیب‌ها با اضافه‌کردن گزینه‌ای برای گزارش سوء استفاده‌ها یا خط مشی‌های تخلفات توسط دیگر کاربران شبکه می‌توانند انجام دهند. در برخی کشورها، شبکه‌های اجتماعی همچون فیسبوک و Bebo یک بخش "Panic Button" را برای حفاظت بهتر از کودکان اضافه کرده‌اند.

۲-۴- تولیدکنندگان محصولات امنیتی حافظ حریم خصوصی

شرکت‌های تجاری مختلف، گزینه‌های امنیتِ اینترنت خود را توسعه داده و در حال حاضر راه‌حل‌های نرم‌افزاری به‌ویژه برای کاربران OSN به‌منظور حفاظت بهتر در برابر تهدیدها پیشنهاد می‌دهند. در این بخش، مسیر نرم‌افزارها و راه‌حل‌های حفاظت از برنامه‌های کاربردی، که توسط شرکت‌های امنیتیِ شناخته‌شده همچون Symantec و Check Point و یا توسط شرکت استارت آپ همچون Online Permissions Technologies، و راه‌حل‌های متن باز همچون NoScript Security Suite توسعه داده شده است، ارائه می‌شود.

راه‌حل‌های امنیت اینترنت: بسیاری از شرکت‌های امنیتی، همچون AVG، Avira، Kaspersky، Panda، McAfee، و Symantec، به کاربران OSN راه‌حل‌های امنیت اینترنت ارائه می‌کنند. این مجموعه نرم‌افزارها نوعاً شامل آنتی ویروس، دیوارهٔ آتش، و دیگر لایه‌های حفاظتی اینترنت است که به کاربران OSN برای محافظت از رایانه‌ها در برابر تهدیدهایی همچون بدافزار، کلیک‌دزدی، و حملات فیشینگ کمک می‌کند. برای مثال، نرم‌افزار امنیت اینترنت McAfee را برای حفاظت کاربرانش در برابر تهدیدهای مختلف همچون بدافزار، بات‌نت‌ها، و سایت‌های نامناسب، فراهم می‌کند.

AVG PrivacyFix: این محصول، نرم‌افزاری است که به‌عنوان یک برنامهٔ تلفن همراه یا افزونه مرورگر وب به کاربران خود راه‌های ساده‌ای برای مدیریت تنظیمات محرمانگی روی فیسبوک، LinkedIn و گوگل پیشنهاد می‌کند. علاوه‌براین، PrivacyFix به کاربرانش در مسدودکردن قریب به ۱۲۰۰ تراکر با دنبال‌کردن تغییر مکان برخط کمک کرده است. این برنامه همچنین به کاربرانش می‌گوید که چه میزان سود برای Facebook و گوگل تولید کرده‌اند.

FB Phishing Protector: این محصول یک افزونه فایرفاکس است که به کاربران فیسبوک در زمان تشخیص فعالیت مشکوک هشدار می‌دهد، مانند تلاش برای حمله script-injection. این افزونه حفاظت در برابر حملات مختلف فیشینگ را نیز فراهم می‌آورد.

Norton Safe Web: محصول شرکت Symantec برنامه‌ای فیسبوکی با بیش از پانصدهزار کاربر است. این برنامه فیدهای خبری کاربران فیسبوک را می‌خواند و به کاربر درباره پیوندها و سایت‌های ناامن هشدار می‌دهد.

McAfee Social Protection: این برنامه یک برنامه تلفن همراهی است که کاربران فیسبوک را قادر به حفاظت از عکس‌های به‌اشترک گذاشته‌شدهٔ خود می‌سازد؛ بدین صورت که می‌تواند دقیقاً مشخص کنند چه اشخاصی بتوانند کدام عکس‌ها را ببینند.

MyPermissions: این خدمت متعلق به شرکت Online Permissions Technology یک سرویس وبی است که برای کاربران پیوندهای مناسبی را به صفحات مجوزدار بسیاری از OSNها همچون فیسبوک، توئیتر، و LinkedIn فراهم می‌کند. این پیوندها به کاربران در دیدن و رد مجوزهایی که در گذشته به برنامه‌های مختلف داده‌اند، به‌منظور حفاظت از محرمانگی بهتر کمک می‌کند. علاوه براین، MyPermissions به‌صورت دوره‌ای رایانامه‌های یادآوری را ارسال وکاربران را برای بررسی تنظیمات مجوزهای OSN ترغیب می‌کند.

NoScript Security Suite: این محصول افزونهٔ متن‌باز برای مرورگرهای مبتنی بر Mozilla مانند فایرفاکس است، که به کاربران اجازه محتوای وب قابل اجرا همچون جاوااسکریپت، جاوا، و فلش را برای اجرا تنها از دامنه‌های مورد اعتماد انتخاب‌شده می‌دهد. مسدودکردن محتوای وب قابل اجرا از سایت‌های غیر قابل اعتماد کاربران OSN را از حملات کلیک‌دزدی و XSS می‌تواند محافظت کند.

Privacy Scanner for Facebook: این محصول متعلق به شرکت Trend Micro برنامه اندرویدی است که تنظیمات محرمانگی کاربر را پویش کرده و خطرات تنظیماتی را که ممکن است منجر به ازدست‌دادن محرمانگی شود، شناسایی و سپس به کاربر در تثبیت تنظیمات کمک می‌کند.

Defensio: سرویس‌دهنده Defensio متعلق به شرکت Websense به محافظت از کاربران شبکه‌های اجتماعی از تهدیدهایی همچون پیوند به بدافزارها کمک می‌کند، که می‌تواند در صفحه فیسبوک کاربر پست شود. این سرویس همچنین در جلوگیری از نشت اطلاعات توسط کنترل محتوای منتشرشدهٔ کاربر با حذف لغات مشخصی از پست‌ها یا فیلترینگ کامنت‌های خاص کمک می‌کند.

ZoneAlarm Privacy Scan: این محصول متعلق به شرکت Check Point برنامه فیسبوکی است که فعالیت‌های اخیر در حساب فیسبوک کاربر را برای تشخیص مسائل محرمانگی و کنترل آنچه دیگران می‌توانند ببینند، بررسی می‌کند. برای نمونه، این محصول پست‌هایی را که در معرض اطلاعات خصوصی کاربر می‌باشد، می‌تواند شناسایی کند.

Net Nanny: این نرم‌افزار متعلق به شرکت ContentWatch به والدین در حفاظت از کودکانشان در برابر محتوای آسیب‌رسان کمک می‌کند. Net Nanny به والدین اجازه نظارت بر فعالیت کودکانشان را در رسانه اجتماعی روی وب‌سایت‌های مختلف OSN همچون فیسبوک، توئیتر، و Flickr می‌دهد.

MinorMonitor: این وب‌سرویس متعلق به شرکت Infoglide یک خدمت کنترل والدین است که به والدین یک دید سریع از فعالیت‌های فیسبوکی کودکان و دوستان برخط می‌دهد. با استفاده از آن، والدین درباره محتوای مشکوک مربوط به کودکانشان می‌توانند آگاه شوند؛ و دوستان غیر هم سن و سال موجود در فهرست دوستان فیسبوکی کودکشان را شناسایی کنند.

۳-۴- پژوهش‌ها

مطالعات انجام‌شدهٔ اخیر، راه‌کارهایی برای تهدیدهای مختلف OSN ارائه کرده است. این راه‌کارها در درجهٔ نخست در شناسایی کاربران و برنامه‌های مخرب تمرکز کرده‌اند. در این بخش، پژوهش‌هایی معرفی می‌شود که راه‌کارهایی برای بهبود تنظیمات محرمانگی کاربران OSN در تشخیص فیشینگ، تولیدکنندگان هرزمحتوا، نمایه‌های جعلی و المثنی، socware و برای جلوگیری از نشت اطلاعاتی و مکانی ارائه کرده‌اند. این راه‌حل‌ها روش رفتار با تهدیدهای شبکه‌های اجتماعی را فراهم می‌کند؛ به‌گونه‌ای که توسط اپراتورهای OSN برای بهبود امنیت و محرمانگی کاربران، توسط شرکت‌های امنیتی برای پیشنهاد بهتر امنیت OSN به مشتریان، یا کاربرانی که می‌خواهند از خود بهتر محافظت کنند، می‌توانند استفاده شوند.

بهبود واسط‌های تنظیم محرمانگی: در سال‌های اخیر پژوهش‌های مختلف روش‌ها و برنامه‌هایی را به کاربران پیشنهاد داده‌اند تا به آنها در فهم بهتر و بهبود تنظیمات محرمانگی شبکهٔ اجتماعی کمک کند. Lipford و همکارانش [۴۷] واسطی برای فیسبوک معرفی کردند که کاربران را قادر به دیدن نمایهٔشان از دید سایر کاربران فیسبوک چه از دید یک دوست و چه از دید یک فرد به‌طورکامل ناشناس می‌کرد. این نوع واسط به کاربران OSN در فهم دقیق اینکه آیا جزئیات شخصی برای دیگر کاربران قابل مشاهده است و همچنین تغییر تنظیمات محرمانگی برطبق آن می‌تواند کمک کند. Fang و LeFevre [۴۸] الگویی برای طراحی یک راهنمای محرمانگی شبکهٔ اجتماعی برای OSNها به‌منظور پیکربندی خودکار تنظیمات محرمانگی کاربر با کمترین تلاش از طرف وی ارائه کردند. Fang و LeFevre همچنین یک نمونه راهنمای محرمانگی برمبنای الگوی کلی خودشان ارائه کردند. راهنمای نمونه از الگوریتم‌های یادگیری استفاده می‌کرد و نتایج نشان می‌داد با وجود کم‌شدن دخالت کاربر در تنظیمات محرمانگی، پیکربندی محرمانگی به‌خوبی پیاده‌سازی شده است. در ۲۰۱۲، Fire و همکارانش [۴۹] افزونه محافظ محرمانگی اجتماعی را معرفی کردند که می‌توانست به کاربران فیسبوک در تنظیم محرمانگی با تنها یک کلیک ساده کمک کند، این کار براساس الگوهای کاربردی تنظیم محرمانگی‌های مختلفِ از پیش تعریف‌شده انجام می‌شد. همچنین در ۲۰۱۲، Paul و همکارانش [۵۰] واسط محرمانگی C4PS را پیشنهاد کردند که از اصول ساده کدگذاری رنگ برای برجسته‌کردن هر ویژگی در نمایه کاربر با یک رنگ خاص وابسته به گروه افرادی که به این ویژگی دسترسی دارند، استفاده می‌کرد. علاوه‌براین، واسط به کاربران امکان تغییر تنظیمات محرمانگی برای یک ویژگی خاص با یک کلیک ساده روی دکمه‌هایی را که نزدیک ویژگی خاص قرار داشت، می‌داد.

تشخیص فیشینگ: پژوهش‌های بسیاری روش‌های ضد فیشینگ مختلفی را برای شناسایی و جلوگیری از حملات فیشینگ پیشنهاد داده‌اند. بیش‌تر این روش‌ها براساس روش‌هایی است که برای شناسایی وب سایت‌ها و URLهای فیشینگ تلاش می‌کنند [۵۱]. با افزایش تعداد حملات فیشینگ در OSNها، پژوهش‌گران راه‌حل‌های اختصاصی را

برای شناسایی حملات فیشینگ شبکه اجتماعی پیشنهاد داده‌اند. در ۲۰۱۲، Lee و همکارانش [۵۲] WarningBird را معرفی کردند، یک سامانهٔ تشخیص URLهای مشکوک برای توئیتر که می‌تواند حملات فیشینگِ پنهان‌شده توسط URLهای تغییر جهت داده‌شده را شناسایی کند. بعدها در همین سال، Aggarwal و همکارانش [۵۳] روش PhishAri را ارائه کردند، که می‌توانست با استفاده از ویژگی‌های خاص توئیتر همچون سن حساب کاربری و تعداد دنبال‌کننده‌های کاربری که پست مشکوک را توئیت کرده، تشخیص دهد که آیا توئیت پست‌شده با یک URL حمله فیشینگ هست یا خیر.

تشخیص تولیدکننده هرزمحتوا: پژوهش‌گران بسیاری راه‌حل‌هایی برای تشخیص تولیدکننده هرزمحتوا در OSNها ارائه کرده‌اند. Benevenuto و همکارانش الگوریتم‌هایی برای تشخیص تولیدکنندگان هرزمحتوای ویدئویی پیشنهاد کردند که در شناسایی تولیدکنندگان هرزمحتوا در میان کاربران YouTube موفق بود. DeBarr و Wechsler [۵۴] از معیار گراف برای پیش‌بینی احتمال ارسال هرزمحتوا توسط کاربر استفاده کردند. Wang [۵۵] روشی برای دسته‌بندی تولیدکنندگان هرزمحتوا در توئیتر با استفاده از ویژگی محتوا و گراف شبکهٔ اجتماعی ارائه کردند. Stringhini و همکارانش [۵۶] بیش از سیصد نمایه جعلی (که "honey-profiles" نیز نامیده می‌شود) در توئیتر، فیسبوک، و MySpace ایجاد کردند و با موفقیت تولیدکنندگان هرزمحتوایی که پیام‌های هرزمحتوا را به نمایه‌های جعلی ارسال می‌کردند، شناسایی کردند. Lee و همکارانش [۱۵] همچنین روشی برای تشخیص تولیدکنندگان هرزمحتوای اجتماعی از انواع مختلف با استفاده از honeypotهای ترکیب‌شده با الگوریتم‌های یادگیری ماشین به‌دست آوردند. در ۲۰۱۳، Aggarwal و همکارانش [۵۷] الگوریتم‌های یادگیری ماشین برای تشخیص انواع مختلفی از تولیدکنندگان هرزمحتوا در Foursquare ارائه کردند. درهمین‌اواخر، Bhat و Abulaish [۱۴] یک چارچوب مبتنی بر اجتماع برای شناسایی تولیدکنندگان هرزمحتوای OSN معرفی کردند. همچنین، Verma و همکارانش [۵۸] یک بررسی که مروری بر روش‌های موجود برای تشخیص کاربران هرزمحتوا در توئیتر بود ارائه کردند.

تشخیص نمایه‌های ثانویه: Kontaxis [۲۰] روشی را برای تشخیص نمایه‌های ثانویه شبکه اجتماعی پیشنهاد دادند. آنها نمونه اولیه‌ای طراحی و پیاده‌سازی کردند که می‌توانست برای بررسی اینکه به کاربران حمله ثانویه شده‌اند یا نه به‌کار گرفته شود. در ۲۰۱۳، Shan و همکارانش [۵۹] CloneSpotter را ارائه کردند که می‌توانست در زیرساخت OSN مستقر شود و حملات ثانویه را با استفاده از داده‌های ثبت‌شده از کاربران تشخیص دهد، مانند IP ورود ثبت‌شدهٔ کاربر که برای اپراتور OSN در دسترس هستند.

تشخیص نمایهٔ جعلی: در سال‌های اخیر، پژوهش‌گران الگوریتم‌ها، روش‌ها، و ابزارهایی برای شناسایی نمایه‌های جعلی و جلوگیری از حملات Sybil مختلف از طریق OSNها توسعه داده‌اند. Yu و همکارانش پروتکل غیرمتمرکز SybilGuard را برای کمک در جلوگیری حملات Sybil و بعدها، Yu و همکارانش پروتکل SybilLimit را نیز ارائه کردند؛ یک سازوکار دفاع در برابر حملات Sybil با استفاده از شبکه‌های اجتماعی. Danezis و Mittal الگوریتم دفاعی SybilInfer را پیشنهاد دادند که می‌توانست میان کاربران "درست‌کار" و "متقلب" تمایز قائل شود. در چنین سالی، Tran و همکارانش سامانهٔ دفاعی SumUp Sybil را برای محدودکردن تعداد آرای جعلی ریخته‌شده توسط sybilها ارائه کردند.

در ۲۰۱۲، Cao و همکارانش ابزار SybilRank را معرفی کردند که از ویژگی‌های گراف OSN برای رتبه‌دهی به کاربران براساس احتمال شناسایی جعلی‌بودن استفاده می‌کرد؛ سپس، آنها SybilRank را در مرکز عملیات Tuenti توسعه دادند؛ بزرگ‌ترین OSN در اسپانیا، و برآورد کردند که به‌طورتقریبی ۹۰٪ از دویست‌هزار کاربرانی که پایین‌ترین رتبه را دریافت کرده‌اند درحقیقت نمایه‌های جعلی هستند. در همان سال، Wang و همکارانش سامانهٔ تشخیص نمایه‌های جعلی جمع‌سپاری را ارائه و با استفاده از داده‌های فیسبوک و Renren (یک OSN چینی)، آن را ارزیابی کردند. همچنین، Fire و همکارانش الگوریتمی برای شناسایی نمایه‌های مخرب با استفاده از ویژگی‌های توپولوژیکی خود شبکهٔ اجتماعی به‌دست آوردند. آنها روش خود را در سه OSN –Academia.edu، Anybeat ، و گوگل+ – آزمایش کردند و در شناسایی نمایه‌های جعلی و تولیدکنندگان هرزمحتوا موفق شدند. Fire و همکارانش همچنین برنامه حفاظت محرمانگی اجتماعی را ارائه کردند که به کاربران فیسبوک در تشخیص نمایه‌های جعلی میان دوستانشان کمک می‌کرد. آنها از مجموع داده‌های ایجادشده توسط برنامه

حفاظت از محرمانگی اجتماعی استفاده کردند و دسته‌بندی یادگیری ماشینی را توسعه دادند که می‌توانست نمایه‌های جعلی را در فیسبوک تشخیص دهد. درهمین‌اواخر، Wang و همکارانش سامانه‌ای ارائه کردند که می‌توانست نمایه‌های جعلی برمبنای تحلیل مدل کلیک‌ها تشخیص دهد. علاوه‌براین راجع به راه‌حل‌های تشخیص حملات Sybil توسط Levine و همکارانش [۶۰] و Hoffman و همکارانش [۶۱] بررسی‌هایی انجام شده‌است.

تشخیص socware: در سال‌های اخیر، مطالعاتی برای فهم و تشخیص بهتر socwareها انجام شده است. در ۲۰۱۲، Rahman و همکارانش برنامه فیسبوکی MyPageKeeper را ارائه کردند که هدف آن حفاظت از کاربران فیسبوک از پست‌های آسیب‌رسان در تایم‌لاین با دسته‌بندی محتوای پست‌های اجتماعی بود. Rahman و همکارانش همچنین Facebook's Rigorous Application Evaluator (FRAppE) را برای تشخیص برنامه‌های مخرب در فیسبوک ارائه کردند. در ۲۰۱۳، Huang و همکارانش اکوسیستم socware را مطالعه کردند و درباره مشخصات انتشار socware نتایجی به‌دست آوردند که در پژوهش‌های آینده تشخیص و جلوگیری انتشار socware می‌تواند کمک کند.

جلوگیری از نشت اطلاعاتی و مکانی: در مطالعات نشت محرمانگی در توئیتر، Mao و همکارانش سرویس "guardian angel service" را ارائه کردند که بر توئیت‌های کاربران می‌تواند نظارت کند و به کاربران احتمال نقض محرمانگی را هشدار دهد. راه حل پیشنهادی آنها بر مبنای دسته‌بندی‌های ساخته‌شده در طول پژوهش می‌تواند باشد که قادر است، توئیت‌های شامل اطلاعات محرمانگی همچون برنامه‌های سفر در تعطیلات را شناسایی کند. علاوه براین، Gomez-Hidalgo و همکارانش [۶۲] از الگوریتم‌های Named Entity Recognition (NER) برای جلوگیری از نشت داده‌ها استفاده کردند. در این مطالعه، آنها یک نمونهٔ اولیه برای تشریح چگونگی روش ارائه‌شده در جلوگیری از نشت داده‌ها فراهم کردند. روش‌های آنها همچنین این امکان را دارد تا برای جلوگیری از افشای مکان کاربران OSN استفاده شود. درهمین‌اواخر، Ghiglieri و همکارانش [۶۳] ابزار Personal DLP را برای کمک به فهم بهتر کاربران OSN و ارزیابی حساسیت وضعیت پست‌ها ارائه کردند. این پژوهش شامل ۲۲۱ شرکت‌کننده بود، و نمونه اولیه Personal DLP تأثیر مثبتی در آگاهی محرمانگی کاربران داشت.

۴-۴- دفاع در عمق در شبکه‌های اجتماعی

بهترین راه حفاظت کاربران OSN از تهدیدهای ذکرشده در بخش قبل توسط اپراتورهای OSN، شرکت‌های امنیتی تجاری، و پژوهش‌گران به کاربران OSN ارائه شده است. همانند راه‌کارهای امنیتی دنیای واقعی، این راه‌کارها برای کاربران OSN با چندین لایهٔ حفاظتی در برابر این تهدیدها می‌تواند فراهم شود. در ادامه مکان قرارگیری راه‌کارهای ارائه‌شده در ساختار شبکهٔ اجتماعی جهت حفاظت بهتر از کاربران ارائه شده است.

نخستین لایهٔ امنیتی، که مشابه عملکرد قفل درب ورودی است، برای جلوگیری از مزاحمان ناخواسته از ورود و دیدن پست‌ها و جزئیات شخصی کاربران OSN است. این لایه شامل تنظیمات مختلف محرمانگی و امنیتی پیشنهادشده توسط اپراتورهای مختلف OSN است. با این حال، در موارد بسیاری اغلب کاربران OSN آشنا یا آگاه از بهترین راه برای قفل‌کردن نمایه خود نیستند، درعوض تنظیمات محرمانگی خود را به‌صورت پیش‌فرض رها می‌کنند، که اغلب محافظت ناکافی را به همراه دارد. برای کمک به چنین کاربرانی، شرکت‌های امنیتی و پژوهش‌گران راه‌حل‌هایی را توسعه داده‌اند، همچون پویش‌گر پنهانی برای فیسبوک، پویش‌گر پنهانی ZoneAlarm، و پشتیان محرمانگی اجتماعی، که تمام موارد ذکرشده به کاربران OSN در بهبود تنظیمات محرمانگی می‌تواند کمک کند. با این وجود، در بسیاری از موقعیت‌های دنیای واقعی، کاربران OSN قفل‌زدن به درب را فراموش می‌کنند، و در نتیجه ممکن است، اطلاعات حساس دربارهٔ خودشان، همچون برنامهٔ سفرهای تعطیلات در آینده یا وضعیت سلامتی نشت کند. برای جلوگیری از این نوع افشای اطلاعات، پژوهش‌گران و شرکت‌های امنیتی راه‌حل‌هایی پیشنهاد می‌دهند که به‌صورت خودکار اطلاعات پست‌شدهٔ کاربران را پویش و از اشترک‌گذاری پست‌های حاوی اطلاعات حساس جلوگیری می‌کند.

دومین لایه حفاظتی مشابه عملکرد هشدار امنیتی و هدف از آن جلوگیری کاربران مخرب از جمع‌آوری پست‌ها و جزئیات شخصی کاربران OSN است و مانع هک دستگاه‌ها و حساب‌های شبکهٔ اجتماعی کاربران ناآگاه در میان کاربران مخرب می‌شود. این لایه شامل راه‌حل‌های مختلف امنیت تجاری اینترنت، به‌علاوه فیشینگ‌های مختلف، نمایه‌های جعلی، و راه‌حل‌های تشخیص socware پیشنهادشده توسط

پژوهش‌گران است که کاربران OSN می‌توانند خود آن را نصب کنند. این نوع از راه‌حل‌ها برای تشخیص تهدیدهای فعال می‌تواند بسیار مؤثر باشد، که در برخی موارد برای آلوده‌کردن بسیاری از کاربران OSN تلاش می‌کنند. در بیشتر موارد، این راه‌حل‌ها برای شناسایی تهدیدهای هدف‌مندتر ناکافی است؛ مانند حملات de-anonymization، شناسایی حملات نمایهٔ المثنی، حملات استنتاجی ناشی از نشت اطلاعات، و شکارچیان برخط، که تمام آنها افرادِ هدفی را با استفاده از OSN انتخاب می‌کنند.

لایهٔ حفاظتی سوم، که مانند یک دوربین امنیتی عمل می‌کند، یک لایهٔ امنیتی ویژهٔ کودکان و OSN مورد استفاده آنها است. هدف از این لایه حفاظت از کودکان و نوجوانان با دادن قابلیت نظارت فعالیت برخط در درجه نخست از طریق نرم‌افزار نظارتی مختلف مانند Net Nanny و MinorMonitor به والدین است. این راه حل به والدین در حفاظت از کودکانشان از تهدیدهای هدف‌دار مانند شکارچی‌های برخط و مزاحمت سایبری می‌تواند کمک کند.

لایهٔ حفاظتی چهارم، که به عملکرد نگهبان محله می‌توان تشبیه کرد، از گزارش‌های دریافتی برای اشارهٔ دقیق به کاربران مخرب در OSN استفاده می‌کند. این لایه شامل راه‌حل‌های مختلف همچون گزینه‌ای برای گزارش درباره دیگر کاربران شبکه اجتماعی به یک اپراتور OSN است. کاربران OSN با یکدیگر برای شناسایی تهدیدهایی همچون نمایه‌های جعلی، کلیک‌دزدی، کلاه‌برداری اینترنتی، socware، و مزاحمت سایبری، می‌توانند همکاری کنند و این موارد را به اپراتورهای OSN گزارش دهند.

لایهٔ پنجم حفاظتی، که مشابه نیروهای پلیس عمل می‌کند، شامل سازوکارهای احراز هویت است که برای اطمینان از ورود یک فرد واقعی به OSN است. سازوکارهای احراز هویت می‌توانند در تشخیص کاربران مخرب همانند socialbotها، کمک‌کننده باشند، و از ورود آنها به OSN و حمله به دیگر کاربران شبکه اجتماعی جلوگیری کند. علاوه‌براین، به‌دلیل دسترسی به‌طورتقریبی نامحدود به داده‌های کاربران OSN، metadata، و فعالیت‌ها، اپراتور OSN بسیاری از تهدیدهای بالقوه را براساس توپولوژی کامل شبکه اجتماعی، همراه با نشانی IP کاربران، زمان‌های ورود، و الگوهای رفتاری، که در بیشتر موارد تنها برای اپراتور OSN در دسترس است، می‌تواند شناسایی کند. به‌علاوه، همان‌طورکه در بخش‌های قبل شرح داده شد، به‌کارگیری مجموعه داده‌های واحد به محافظت کاربران OSN از تهدیدهایی همچون حملات فیشینگ، تولیدکنندگان هرزمحتوا، حملات المثنی، و نمایه‌های جعلی می‌تواند کمک کند. Fire و همکارانش نشان دادند که چگونه اپراتور OSN از تمام توپولوژی گراف شبکه اجتماعی به‌منظور تشخیص نمایه‌های جعلی و تولیدکنندگان هرزمحتوا می‌تواند بهره بگیرد. علاوه‌براین، همان‌طورکه توسط Stringhini و همکارانش شرح داده شد، اپراتور OSN از کنترل خود برای پخش‌کردن " honey-profiles" بسیاری می‌تواند استفاده کند که در تشخیص کاربران مخرب همچون تولیدکنندگان هرزمحتوا می‌تواند مؤثر باشد.

این پنج لایهٔ امنیتی می‌تواند به کاربران OSN حفاظت در برابر تقریباً تمام تهدیدهای توصیف‌شده در بخش قبل بدهد؛ مضاف بر این‌که، اگر کاربران OSN تنها از سه لایهٔ نخست استفاده کنند، امنیتشان در برابر بیشتر تهدیدهای توصیف‌شده در بالا تأمین می‌شود. با این اوصاف، اپراتورهای OSN –به‌منظور کنترل شبکه، به تمام داده‌های و ابرداده‌های کاربران دسترسی واحدی دارند–در بهترین موقعیت برای بهبود امنیت و محرمانگی کاربرانشان هستند.

۵- راه‌کارهای پیش‌گیری از تهدیدهای شبکه‌های اجتماعی

همان‌طورکه در سراسر این پژوهش شرح داده شد، کاربران OSN با تهدیدهای محرمانگی و امنیتی مختلف و شایعی روبه‌رو می‌شوند. خوشبختانه، راه‌حل‌ها و روش‌های نرم‌افزاری بسیاری امروزه وجود دارد که به کاربران OSN در دفاع بهتر در مقابل تهدیدها می‌تواند کمک کند. در این بخش، چند روش با کاربری آسان ارائه می‌شود که به کاربران OSN در بهبود امنیت و محرمانگی در شبکه‌های اجتماعی همچون فیسبوک و توئیتر می‌تواند یاری رساند. به کاربران OSN توصیه می‌شود، برای حفاظت بهتر خود در این بسترها هشت پیشنهاد ارائه‌شده در زیر را در هر حساب OSN خود به‌کار گیرند:

۱) حذف اطلاعات شخصی غیر ضروری: به کاربران OSN توصیه می‌شود مروری بر جزئیات اطلاعاتی که در حساب‌های OSN خود دارند، انداخته و اطلاعات غیرضروری دربارهٔ خود، خانواده، و دوستانشان را حذف کنند. همچنین پیشنهاد می‌شود که در صورت امکان

کاربران فهرست دوستان خود را برای جلوگیری از حمله استنتاجی پنهان نگه‌دارند . علاوه براین، به کاربران توصیه می‌شود در زمان استفاده از OSN از نام کامل خود به منظور جلوگیری از تشخیص چهره استفاده نکنند، پیشنهاد خیلی بالاتر عدم استفاده از تصویر قابل شناسایی در عکس نمایه است.

۲) درست‌کردن تنظیمات امنیتی و محرمانگی: در بسیاری از شبکه‌های اجتماعی، همچون فیسبوک، تنظیمات محرمانگی پیش‌فرض ناکافی هستند. در عین حال پژوهش‌های اخیر نشان داده است که بسیاری از کاربران فیسبوک تمایل به باقی‌ماندن تنظیمات پیش‌فرض خود دارند [۶۴]. به‌منظور محافظت بهتر کاربران در فیسبوک و دیگر OSNها، تغییر تنظیمات محرمانگی پیشنهاد می‌شود؛ به‌گونه‌ای که اطلاعات شخصی کاربران تنها برای خودشان، یا درنهایت تنها دوستانشان قابل رؤیت باشد. علاوه براین، در صورت امکان توصیه می‌شود، کاربران گزینه مرور امن و دیگر سازوکارهای احراز هویت دردسترس همچون احراز هویت دو عاملی توئیتر را فعال کنند.

۳) نپذیرفتن درخواست‌های دوستی از افراد ناشناس: همان‌طورکه در بخش پیشین شرح داده شد، نمایه‌های جعلی، رایج و اغلب خطرناک هستند. بنابراین، اگر کاربری درخواست دوستی را از شخص ناشناس دریافت کند، توصیه می‌شود، چنین درخواست‌هایی را رد کند و نپذیرد. اگر کاربر نامعلوم است و نظر به تأیید درخواست دوستی دارید، توصیه می‌شود یک بررسی پیش‌زمینه‌ای کوتاهی در دوستان جدید، و دست‌کم، تصویر نمایه دوست را در جستجوی عکس گوگل وارد کنید و نام کامل دوست مورد نظر و دیگر جزئیات را در دیگر موتورهای جستجو به‌منظور تأیید هویت فرد وارد کنید. به‌منظور شناسایی و حذف افراد ناشناس که در فهرست دوستان کاربر وجود دارد، به کاربران OSN پیشنهاد می‌شود، فهرست دوستان خود را امتحان یا از برنامه‌هایی همچون پشتیبان امن اجتماعی استفاده و به‌صورت دوره‌ای دوستانی که با آنها آشنا یا دوست نبوده و حق دسترسی به اطلاعات شخصی را نداشته حذف کنند.

۴) نصب نرم‌افزار امنیت اینترنت: به کاربران OSN توصیه می‌شود، دست‌کم یکی از چندین محصول نرم‌افزاری امنیت اینترنت را نصب کنند. فیسبوک بارگیری رایگان انواع مختلف از این نرم‌افزارها را پیشنهاد می‌کند. همچنین کاربران برای نصب دیگر محصولات محرمانه و امنیتی شرح‌دادشد در بخش‌های قبل توصیه می‌شود.

۵) حذف برنامه‌های شخص سوم نصب‌شده: بسیاری از کاربران نمی‌دانند که برنامه‌های شخص سوم اغلب داده‌های شخصی برخط را جمع‌آوری می‌کند. مطالعه اخیر نشان می‌دهد که ۳۰٪ گروه‌های آزمایش‌شده کاربران فیسبوکی دست‌کم چهل برنامه نصب‌شده روی حساب‌های کاربری دارند. به کاربران توصیه می‌شود، برنامه جدید غیرضروری نصب نکنند. علاوه براین، به کاربران توصیه می‌شود، به‌صورت دوره‌ای به فهرست برنامه‌های نصب‌شده خود رفته و هر برنامه غیرضروری را حذف کنند.

۶) عدم انتشار موقعیت مکانی: همان‌طورکه شرح داده شد، بسیاری از کاربران مکان فعلی و آینده خود در چندین OSN منتشر می‌کنند؛ که این اطلاعات توسط مجرمان و کلاه‌برداران مورد استفاده می‌تواند قرار گیرد. پیشنهاد می‌شود، کاربران از انتشار هرگونه موقعیت جغرافیایی خودداری کنند. علاوه‌براین، به کاربران توصیه می‌شود، برچسب مکان جغرافیایی روی دستگاه‌های موبایل خود و دوربین‌ها را برای جلوگیری از به‌اشترک‌گذاری عکس و ویدئویی که ممکن است حاوی اطلاعات مکانی باشد، غیرفعال کنند.

۷) به دوستان OSN خود اعتماد نکنید: کاربران OSN تمایل به اعتماد به دوستان در شبکهٔ اجتماعی دارند. از آنجایی که این اعتماد نابه‌جا می‌تواند باشد، به کاربران OSN توصیه می‌شود، اقدامات احتیاطی اضافی را در زمان ارتباط با دوستان برخط خود رعایت کنند. به کاربران همچنین سفارش می‌شود، پیش از ارائه هرگونه اطلاعات حساس و شخصی درباره خود دوباره فکر کنند، حتی زمانی که عکسی را پست می‌کنند. کاربران OSN می‌بایست به‌جد از آشکارکردن نشانی محل سکونت، شماره تلفن، یا شماره کارت‌های اعتباری اجتناب کنند.

۸) نظارت بر فعالیت کودکان در OSN: به والدین توصیه می‌شود، تمام سفارش‌های ذکرشده در بالا را برای نمایه‌های OSN کودکانشان رعایت کنند. علاوه‌براین، به والدین نظارت بر فعالیت‌های برخط در OSN پیشنهاد می‌شود. این نظارت به‌صورت دستی یا توسط یکی از محصولات نرم‌افزاری نظارتی، می‌تواند انجام شود.

همچنین، توصیه اکید می‌شود که والدین و کودکانشان به‌صورت دوره‌ای با یکدیگر فهرست دوستان را برای حذف دوستان ناشناس بررسی کنند.

۶- نتیجه‌گیری

در این مقاله به معرفی تهدیدهای شبکه‌های اجتماعی و راه‌کارهای موجود برای آنها پرداختیم. برای این تهدیدها راه‌کارهایی وجود دارد، و مجموعه راه‌حل‌هایی ارائه شده‌اند که به حفاظت از امنیت و محرمانگی OSN کمک می‌کند. با این وجود، راه‌کارهای ارائه‌شده حفاظت کامل از امنیت و محرمانگی کاربر را نمی‌توانند فراهم آورد. به‌منظور محافظت خوب در برابر تهدیدهای مختلف برخط، کاربران باید مراقب اطلاعات برخط پست‌شده باشند، و باید بیش از یک راه‌کار را به‌کار گیرند. در موارد بسیاری، کاربران باید هم برای محافظت بهتر از محرمانگی و هم شناسایی تهدیدهای بالقوه به‌دنبال یک ابزار واسط OSN باشند.

۷- مراجع

[1] Facebook. Facebook Reports Fourth Quarter and Full year 2013 Results. Retrieved 21/04/2016, from http://investor.fb.com/releasedetail.cfm?ReleaseID=821954

[2] Facebook. Form 10-k (Annual Report)—Filed 02/01/13 for the Period Ending 12/31/12. Retrieved 21/04/2016, from http://files.shareholder.com/downloads/AMDA-NJ5DZ/2301311196x0xS1326801-13-3/1326801/1326801-13-3.pdf

[3] Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). *The socialbot network: when bots socialize for fame and money* .Paper presented at the Proceedings of the 27th Annual Computer Security Applications Conference.

[4] Stringhini, G., Wang, G., Egele, M., Kruegel, C., Vigna, G., Zheng, H., & Zhao, B. Y. (2013). *Follow the green: growth and dynamics in twitter follower markets.* Paper presented at the Proceedings of the 2013 conference on Internet measurement conference.

[5] Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2013). Design and analysis of a social botnet. *Computer Networks, 57*(2), 556-578 .

[6] Dwyer ,C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339 .

[7] Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sha-ring, and privacy on the Facebook.* Paper presented at the Privacy enhancing tech-nologies.

[8] Elyashar, A., Fire, M., Kagan, D., & Elovici, Y. (2013). *Homing socialbots: intrusion on a specific organization's employee using Socialbots.* Paper presented at the Proceed-ings of the 2013 IEEE/ACM Inter-national Conference on Advances in Social Networks Analysis and Mining.

[9] Miller, C. C. (2013). Tech Companies Concede to Surveillance Program. Retriev-ed 21/04/2016, from http://www.ny-times.com/2013/06/08/technology/tech-companiesbristling-concede-to-government-surveillance-efforts.html

[10] Constine, J. (2012). Facebook Launches Verified Accounts and Pseudonyms. Ret-rieved 21/04/2016, from http://tech-crunch.com/2012/02/15/facebook-verified-accounts-alternate-names/

[11] O'Leary, J. (2013). Getting Started With Login Verification. Retrieved 21/04/2016, from https://blog.twitter.com/2013/getting-started-login-verification

[12] Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). *Analyzing facebook privacy settings: user expectations vs. reality.* Paper presented at the Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

[13] Singer-Vine, J. A. a. J. (2012). Selling you on facebook. Retrieved 21/04/2016, from http://online.wsj.com/news/articles/SB10001424052702303302504577327744009046230

[14] Bhat, S. Y., & Abulaish, M. (2013). *Community-based features for identifying spammers in online social networks.* Paper presented at the Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.

[15] Lee, K., Caverlee, J., & Webb, S. (2010). *Uncovering social spammers: social honeypots+ machine learning.* Paper pre-sented at the Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval.

[16] Benevenuto, F., Rodrigues, T., Almeida, V., Almeida, J., & Gonçalves, M. (2009). *Detecting spammers and content promoters in online video social networks.* Paper pre-sented at the Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval.

[17] Wang, G., Konolige, T., Wilson, C., Wang, X., Zheng, H., & Zhao, B. Y. (2013). *You are how you click: Clickstream analysis for sybil detection.* Paper presented at the Proc. USENIX Security.

[18] Yu, H., Gibbons, P. B., Kaminsky, M., & Xiao, F. (2008). *Sybillimit: A near-optimal social network defense against sybil attacks.* Paper presented at the Security and Privacy, 2008. SP 2008. IEEE Symposium on.

[19] Fire, M., Kagan, D., Elyashar, A., & Elovici, Y. (2014). Friend or foe? Fake profile identification in online social networks. *Social Network Analysis and Mining, 4*(1), 1-23 .

[20] Kontaxis, G., Polakis, I., Ioannidis, S., & Markatos, E. P. (2011). *Detecting social network profile cloning.* Paper presented at the Pervasive Computing and Communi-cations Workshops (PERCOM Workshops), 2011 IEEE International Conference on.

[21] Facebook. (2013). Facebook Newsroom. Retrieved 26/04/2016, from http://news-room.fb.com/Key-Facts

[22] Aaron, J. B. a. S. (2013). 72% of Online Adults are Social Networking Site Users. Retrieved 26/04/2016, from http://ww-w.pewinternet.org/2013/08/05/72-of-online-adultsare-social-networking-site-users

[23] Nielsen. (2011). State of the Media: The Social Media Report (q3 2011). Retrieved 26/04/2016, from http://cn.ni-elsen.c-om/documents/Nielsen-Social-Media-Report_FINAL_090911.pdf

[24] Fox, Z. (2013). The 10 Most Frequently Used Smartphone Apps. Retrieved 26/04/2016, from http//:mash-able.com/2013/08/05/most-used-smartphone-apps/

[25] S. Livingstone, L. H., and K. Ólafsson. (2011). Eu Kids Online: Final Report.

[26] T. Amin, O. O., J. Lu, and J. An. (2010). Facebook: A Comprehensive Analysis of Phishing on a Social System. Retrieved 26/04/2016, from https://cour-ses.ece.ubc.ca/412/term_project/reports/2010/fa-cebook.pdf

[27] al, D. C. e. (2010). Microsoft Security Intelligence Report Volume 10. Retrieved 26/04/2016, from http://www.micro-soft.com/enus/download/details.aspx?id١٧٠٣٠=

[28] Mills, E. (2009). Facebook Hit by Phishing Attacks for a Second Day. Retrieved 26/04/2016, from http://news.cnet.com/8301-1009_3-10230980-83.html

[29] Chowdhury, A. (2010). State of Twitter Spam. Retrieved 26/04/2016, from h-ttps://blog.twitter.com/2010/state-twitter-spam

[30] Tristan, L. (2013). Twitter's Growing Spam Problem. Retrieved 26/04/2016, from h-ttp://www.forbes.com/sites/tristanlouis/2013/04/07/twitters-growing-spam-problem/

[31] Livshits, V. B., & Cui, W. (2008). *Spectator: Detection and Containment of JavaScript Worms.* Paper presented at the USENIX Annual Technical Conference.

[32] Paul, I. (2009). Twitter worm: A closer look at what happened. *PCWorld, San Francisco, CA, USA, Apr* .

[33])NASAA), N. A. S. A. A. Informed Investor Advisory: Social Networking. Retrieved 29/04/2016, from http://www.na-saa.org/5568/informedinvestoradvisorysocial-networking/

[34] Krishnamurthy, B., & Wills, C. E. (2009). *On the leakage of personally identifiable information via online social networks.* Paper presented at the Proceedings of the 2nd ACM workshop on Online social networks.

[35] Perlroth, N. (2013). Fake twitter followers become multimillion-dollar business. *The New York Times, 5* .

[36] Torabi, S., & Beznosov, K. (2013). *Privacy Aspects of Health Related Information Sharing in Online Social Networks.* Paper presented at the HealthTech.

[37] Humphreys, L., Gill, P., & Krishnamurthy, B. (2010). *How much is too much? Privacy issues on Twitter.* Paper presented at the Conference of International Communication Association, Singapore.

[38] Cheng, Z., Caverlee, J., & Lee, K. (2010). *You are where you tweet: a content-based approach to geo-locating twitter users.* Paper presented at the Proceedings of the 19th ACM international conference on Information and knowledge management.

[39] Friedland, G., & Sommer, R. (2010). *Cybercasing the Joint: On the Privacy Impli-cations of Geo-Tagging.* Paper presented at the HotSec.

[40] Rahman, M. S., Huang, T.-K., Madhyastha, H. V., & Faloutsos, M. (2012). *Efficient and scalable socware detection in online social networks.* Paper presented at the Presented as part of the 21st USENIX Security Symposium (USENIX Security 12).

[41] Rahman, M. S., Huang, T.-K., Madhyastha, H. V., & Faloutsos, M. (2012). *Frappe: detecting*

[52] Lee, S., & Kim, J. (2012). *WarningBird: Detecting Suspicious URLs in Twitter Stream.* Paper presented at the NDSS.

[53] Aggarwal, A., Rajadesingan, A., & Kumaraguru, P. (2012). *PhishAri: Auto-matic realtime phishing detection on twitter.* Paper presented at the eCrime Researchers Summit (eCrime), 2012.

[54] DeBarr, D., & Wechsler, H. (2010). Using social network analysis for spam detection *Advances in Social Computing* (pp. 62-69): Springer.

[55] Wang, A. H. (2010). *Don't follow me: Spam detection in twitter.* Paper presented at the Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on.

[56] Stringhini, G., Kruegel, C., & Vigna, G. (2010). *Detecting spammers on social networks.* Paper presented at the Proceedings of the 26th Annual Computer Security Applications Conference.

[57] Aggarwal, A., Almeida, J., & Kumaraguru, P. (2013). *Detection of spam tipping behaviour on foursquare.* Paper presented at the Proceedings of the 22nd international conference on World Wide Web companion.

[58] Verma, M., & Sofat, S. (2014). Techniques to Detect Spammers in Twitter-A Survey. *International Journal of Computer Appli-cations, 85*(10).

[59] Shan, Z., Cao, H., Lv, J., Yan, C., & Liu, A. (2013). *Enhancing and identifying cloning attacks in online social networks.* Paper presented at the Proceedings of the 7th International Conference on Ubiquitous Information Management and Communi-cation.

[60] Levine, B. N., Shields, C., & Margolin, N. B. (2006). A survey of solutions to the sybil attack. *University of Massachusetts Amherst, Amherst, MA* .

[61] Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. *ACM computing surveys (CSUR), 42*(1), 1 .

[62] Gomez-Hidalgo, J. M., Martin-Abreu, J. M., Nieves, J., Santos, I., Brezo, F., & Bringas, P. G. (2010). *Data leak prevention through named entity recognition.* Paper presented at the Social Computing (SocialCom), 2010 IEEE Second International Conference on.

[63] Ghiglieri, M., Stopczynski, M., & Waidner, M. (2014). *Personal DLP for facebook.* Paper presented at the Pervasive Computing and Communications Workshops (PER-COM Workshops), 2014 IEEE Inter-national Conference on.

malicious facebook applications. Paper presented at the Proceedings of the 8th international conference on Emerging networking experiments and technologies.

[42] Huang, T.-K., Rahman, M. S., Madhyastha, H. V., Faloutsos, M., & Ribeiro, B. (2013). *An analysis of socware cascades in online social networks.* Paper presented at the Proceedings of the 22nd international conference on World Wide Web.

[43] UNICEF. (2011). *Child safety online: Global challenges and strategies*: UNICEF Innocenti Research Centre.

[44] Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online" predators" and their victims: myths, realities, and implications for prevention and treatment. *American Psychologist, 63*(2), 111 .

[45] Lpsos. (2012). One in Ten (12%) Parents Online, Around the World Say Their Child has Been Cyberbullied, 24% Say They Know of a Child Who has Experienced Same in Their Community. Retrieved 29/04/2016, from http://www.ip-sosna.c-om/newspolls/pressrelease.aspx?id=5462

[46] Stein, T., Chen, E & ,.Mangla, K. (2011). *Facebook immune system.* Paper presented at the Proceedings of the 4th Workshop on Social Network Systems.

[47] Lipford, H. R., Besmer, A., & Watson, J. (2008). Understanding Privacy Settings in Facebook with an Audience View. UPSEC ,8, 8-1.

[48] Fang, L., & LeFevre, K. (2010). *Privacy wizards for social networking sites.* Paper presented at the Proceedings of the 19th international conference on World wide web.

[49] Fire, M., Kagan, D., Elishar, A., & Elovici, Y. (2012). *Social privacy protector-protecting users' privacy in social networks.* Paper presented at the SOTICS 2012: Second International Conference on Social Eco–Informatics.

[50] Paul, T., Stopczynski, M., Puscher, D., Volkamer, M., & Strufe, T. (2012). *C4ps: colors for privacy settings.* Paper presented at the Proceedings of the 21st international conference companion on World Wide Web.

[51] Ma, J., Saul, L. K., Savage, S., & Voelker, G. M. (2009). *Beyond blacklists: learning to detect malicious web sites from suspicious URLs.* Paper presented at the Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining.

[64] Lewis, J. (2012). How spies used facebook to steal NATO chiefs' details. Retrieved 29/04/2016, from h-ttp://www.tele-graph.co.uk/technology/9136029/HowspieusedFacebooktostealNatochiefsdetails.html

[65] Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. IEEE network, 24(4).

[66] Cutillo, L. A., Manulis, M., & Strufe, T. (2010). Security and privacy in online social networks. In Handbook of Social Network Technologies and Applications (pp. 497-522). Springer, Boston, MA.

[67] Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security issues in online social networks. IEEE Internet Computing, 15(4), 56-63.

علیـــرضا نوروزی فوق دکترای خود را در رشـــتهٔ فناوری اطلاعات از دانشـــگاه صـنعتی شـریف گرفتهاسـت. وی عضـو هیئت علمی و مشـاور آزاد شـرکتهای فناوری اطلاعات دولتی و خصوصیست. زمینههای پژوهشی ایشان هوش مصنوعی، علوم شناختی، مهندســـی نرمافزار و امنیّت اطلاعات اســـت. وی همچنین بنیانگذار چهار استارتآپ فناوری اطلاعات است و چندین جایزهٔ ملّی و بینالمللی را در کارنامهٔ علمی خود دارد.

کمالالدین قـضاوتی تحصـیلات خود را در مقطع کارشناسی ارشد مهندسی فناوری اطلاعات گرایش امنیت در سال ۱۳۹۵ در دانشگاه صنعتی مالک اشتر به پایان رســاند. زمینه پژوهشـــی مورد علاقه وی امنیت فضای سایبری است.