مروری بر تهدیدات امنیتی در شبکه‌های اجتماعی مجازی

سیده‌فاطمه ترابی [۱]، سیدعلیرضا طباطبایی [۲]

[۱] کارشناسی ارشد، دانشگاه ادیان و مذاهب، ایران
torabi110@mail.um.ac.ir
[۲] عضو هیئت علمی دانشگاه علوم قضائی و خدمات اداری، ایران
tabatabaei@ujsas.ac.ir

چکیده

این مقاله به بررسی شبکه‌های اجتماعی و تهدیدات امنیتی مرتبط با آن‌ها می‌پردازد. با گسترش این شبکه‌ها، فرصت‌هایی نظیر تبادل سریع اطلاعات، تقویت روابط اجتماعی، تبادل فرهنگی و بیان هویت اجتماعی برای کاربران ایجاد شده است؛ اما این بسترها همچنین با چالش‌هایی همچون انتشار اخبار جعلی، نقض حریم خصوصی و تهدیدات امنیتی نیز همراه هستند. به‌منظور مقابله با این تهدیدات، راهکارهای متنوعی از جمله تنظیمات امنیتی، گزارش‌دهی سریع، تأیید هویت دومرحله‌ای و آموزش کاربران پیشنهاد می‌شود. همچنین استفاده از الگوریتم‌های پیشرفته برای شناسایی فعالیت‌های مشکوک و تأسیس قوانین دولتی به‌منظور محافظت از حریم خصوصی کاربران در این مقاله موردبحث قرار می‌گیرد. این پژوهش با رویکرد توصیفی و با استفاده از منابع کتابخانه‌ای انجام شده است و با هدف ارائه درک بهتری از تهدیدات و فرصت‌های موجود در شبکه‌های اجتماعی و همچنین راهکارهایی برای ارتقای امنیت کاربران ارائه‌شده است. نتایج این پژوهش به درک بهتر تهدیدات و فرصت‌های موجود در شبکه‌های اجتماعی و ارائه راهکارهایی برای ارتقای امنیت کاربران کمک خواهد کرد.

کلمات کلیدی: شبکه‌های اجتماعی، تهدیدات سایبری، فرصت‌ها، چالش‌ها، امنیت.

۱ مقدمه

شبکه‌های اجتماعی مجازی به‌عنوان ابزارهای اصلی ارتباطی در دنیای امروز، نقش بسزایی در تبادل اطلاعات و بیان هویت‌های اجتماعی دارند. این شبکه‌ها نه‌تنها امکان ارتباط و تعامل کاربران را فراهم می‌کنند، بلکه چالش‌هایی از جمله انتشار اخبار جعلی و تهدیدات امنیتی را نیز به همراه دارند که نیازمند بررسی دقیق‌تری هستند. انگیزه تحقیق در این حوزه، مشاهده تأثیرات عمیق و چندوجهی شبکه‌های اجتماعی بر زندگی کاربران است. هدف این پژوهش، ارائه درک بهتری از فرصت‌ها و چالش‌های ناشی از استفاده از این شبکه‌ها و همچنین شناسایی و ارائه راهکارهایی برای ارتقا امنیت و بهبود تجربه کاربران در این فضاها است.

نوآوری‌های این پژوهش شامل تحلیل جامع و منسجم فرصت‌ها و چالش‌های موجود در شبکه‌های

اجتماعی مجازی است. با بررسی دقیق ابعاد مختلف این بسترها، چالش‌های امنیتی شناسایی شده و راهکارهای مؤثری برای مقابله با این تهدیدات پیشنهاد شده است. این پژوهش به‌عنوان تلاشی نوآورانه، با تعریف شبکه‌های اجتماعی مجازی به‌عنوان بسترهای دیجیتالی که امکان تبادل اطلاعات و بیان هویت‌های اجتماعی را برای کاربران فراهم می‌آورند، آغاز می‌شود. در ادامه، با مروری جامع و دقیق بر تهدیدات امنیتی و نقض حریم خصوصی در این شبکه‌ها، به واکاوی فرصت‌ها و ظرفیت‌های مثبت آن‌ها پرداخته و در کنار آن، معایب و چالش‌های جدی را که این فضاها به همراه دارند، مورد بررسی قرار می‌دهد. این پژوهش در نهایت، با ارائه راهکارهای عملی و مؤثر، به دنبال ارتقای امنیت و بهبود تجربه کاربران در جهان پرچالش فضای مجازی است.

۲ شبکه‌های اجتماعی مجازی

شبکه‌های اجتماعی به‌عنوان یکی از رسانه‌های اجتماعی به پرداز، جمع‌آوری، ارائه و انتشار اطلاعات اجتماعی چون: نژاد، گرایش جنسی، دوست و همراه، مذهب، فیلم و کتاب‌های موردعلاقه، اخبار روز، عکس و... انتشار و ارسال ویدئو اشاره می‌کنند (نو کاریزی، ۱۳۹۴: ۲۹۳). در تعریفی از شبکه‌های اجتماعی آمده است: «گونه‌ای از رسانه‌های اجتماعی است که امکان دست‌یابی به شکل جدیدی از برقراری ارتباط و به‌اشتراک‌گذاری اطلاعات را در اینترنت فراهم آورده است؛ در واقع شبکه‌های اجتماعی را می‌توان از بسترهای مؤثر در تولید علم، اشتراک عقاید و رشد فردی و اجتماعی دانست و در حال حاضر از شبکه‌های اجتماعی به‌عنوان قوی‌ترین رسانه اجتماعی برخط یاد می‌شود (همان)».

۳ مروری بر بررسی تهدیدهای مختلف امنیت و حریم خصوصی در شبکه‌های اجتماعی آن‌لاین

در جدول ۱ به مروری بر روش‌های موجود در خصوص تهدیدهای مختلف امنیت در شبکه‌های اجتماعی آنلاین پرداخته شده است.

۴ فرصت‌های ایجاد شده توسط شبکه‌های اجتماعی

گسترش این شبکه‌های نوین اجتماعی فضای مناسبی است برای: بیان هویت گروه‌های پراکنده، امکان تبادل فرهنگی، ایجاد فعالیت مدنی برای شهروندان، به اشتراک گذاشتن مطالب با دیگران و پیداکردن هم‌فکر و دوست، ایجاد محیطی برای بیان عقاید و دیدگاه‌های سیاسی و اجتماعی، تبادل سریع اطلاعات و ازدیاد قدرت تحلیل کاربران و تقویت تفکر و روحیه انتقادی، امکان آشنایی و روابط با افراد از فرهنگ‌های متنوع و افکار مختلف، افزایش خرد جمعی عموم کاربران در سطح کلان، تقویت روحیه خلاقیت و ایجاد محیطی برای بیان ایده و نوآوری‌ها به‌صورت آزادانه و آشنایی با افکار و سلائق و نظریان سایر کاربران، افزایش مشارکت و کنش‌های اجتماعی کاربران و ایجاد فضایی برای معرفی و تبلیغ (کارکرد تبلیغی و محتوایی)، ارتقا سرعت در

جدول ۱: مروری بر روش‌های موجود در خصوص حریم خصوصی و امنیت در شبکه‌های اجتماعی آن‌لاین

منبع	مباحث کلیدی مورد بررسی
(راتهور[Rathore] و همکاران، ۲۰۱۷، ۴۳-۶۹)	• بررسی تهدیدهای مختلف به‌اشتراک‌گذاری محتوای چندرسانه‌ای در شبکه‌های اجتماعی آنلاین • ارائه راه‌حل‌های دفاعی پیشرفته • ارائه برخی فن‌های امنیتی
(کایس[Kayes] و آیامنیتچی، ۲۰۱۷، ۱-۲۱)	• طبقه‌بندی مشکلات حریم خصوصی و امنیتی در شبکه‌های اجتماعی آنلاین • بحث در مورد راه‌حل‌های کاهش حملات به شبکه‌های اجتماعی آنلاین • بحث در مورد چالش‌ها و تحقیقات آینده
(پنگ [Peng]، و همکاران، ۲۰۱۸، ۱۷-۳۲)	• مروری بر شبکه های اجتماعی آنلاین، از جمله تعریف و انواع • بحث در مورد تجزیه و تحلیل نفوذ در شبکه های اجتماعی آنلاین • بحث در مورد چالش‌ها و جهت‌گیری‌های تحقیقاتی آینده
(فرگ [Ferrag]، مگلاراس و احمیم، ۲۰۱۷، ۳۰۱۵-۳۰۴۵)	• بررسی مدل‌های حفظ حریم خصوصی شبکه‌های اجتماعی • خلاصه حملات مهم • بحث پیرامون تحقیقات مختلف در حفظ حریم خصوصی
(رامالینگام [Ramalingam]، و چینایاه، ۲۰۱۸، ۱۶۵-۱۷۷)	• نظرسنجی از فن موجود تشخیص پروفایل جعلی ارائه کرد • بحث در مورد تحقیقات موجود در مورد تهدیدات امنیتی شبکه‌های اجتماعی آنلاین • بحث در مورد مسئله تشخیص Sybil
(سرما [Sarmah]، ۲۰۱۸، باتاچاریه و کالیتا: ۱۱۳-۱۴۳)	• ارائه بحث مفصلی در مورد حملات مختلف XSS • ارائه برخی از ابزار تشخیص حمله XSS • بحث در مورد مسائل و چالش‌ها

ادامه جدول ۱

منبع	مباحث کلیدی مورد بررسی
(ساها [Sahoo] و گوپتا. ۲۰۱۹، ۸۳۲-۸۶۴)	• طبقه‌بندی ارائه شده از حملات اخیر شبکه‌های اجتماعی آنلاین و جریان آنها • ارائه گزارش‌های تهدید امنیتی در برنامه‌های کاربردی شبکه‌های اجتماعی • نکات عملی برای محافظت از اطلاعات کاربر در شبکه‌های اجتماعی آنلاین • بحثی پیرامون تحقیقات آینده
(علی [Ali] و همکاران، ۲۰۱۸، ۱۱۴)	• ارائه مسائل رایج امنیت و حریم خصوصی شبکه‌های اجتماعی آنلاین • توصیه‌های امنیتی به کاربران OSN برای محافظت
(گوو [Guo]، و همکاران، ۲۰۲۰: ۱۷۷۰-۱۸۰۶)	• حملات شبکه‌های اجتماعی و جرایم سایبری • سازوکارهای دفاعی همراه با مزایا و معایب • بحث در مورد جهت‌گیری تحقیقاتی آینده با نگرانی‌های قانونی و اخلاقی
(جِین [Jain] و همکاران، ۲۰۲۱، ۲۱۵۷-۲۱۷۷)	• ارائه گزارش‌های آماری از پارامترهای مختلف شبکه‌های اجتماعی آنلاین • مروری بر تهدیدهای مختلف امنیتی و حریم خصوصی • بحث در مورد رویکردهای دفاعی موجود برای تأمین امنیت • بحث در مورد چالش‌ها و دستورالعمل‌های امنیتی
(باتاچاریه [Bhattacharya]، و همکاران، ۲۰۲۳، ۱-۲۸)	• طبقه‌بندی نقض حریم خصوصی و حملات امنیتی به شبکه‌های اجتماعی آنلاین • رویکردهای مبتنی بر یادگیری ماشین موجود برای حل حملات امنیتی

امر آموزش و تسریع ارتباط شاگردان با یکدیگر و با اساتید خود، عبور از مرزهای جغرافیایی و آشنایی با نظرات متفاوت از جوامع مختلف (زارعی، ۱۳۹۶: ۱۲-۱۵؛ ذاکری و رضاپور، ۱۳۹۷: ۷۷-۹۴).

۵ معایب شبکه‌های مجازی

شبکه‌های اجتماعی با معایب متعددی همراه هستند که شامل انتشار سریع اخبار جعلی و شایعات، نقض حریم خصوصی کاربران، تهدیدات امنیتی (مانند هرزنامه[۱]، بدافزارها[۲] و فیشینگ[۳]) (فایر، گلدشمیت و الوویچی، ۲۰۱۴، ۲۰۱۹-۲۰۳۶)، و تبلیغات نادرست می‌شود. این فضاها باعث کاهش تعاملات اجتماعی و افزایش فاصله عاطفی در خانواده‌ها شده و تأثیرات منفی بر رفتار، تحصیل کودکان، و هویت فرهنگی کاربران و تبلیغات نادرست و القای شبهات دارند. همچنین، تهدیدات مدرن مانند حملات شبیه‌سازی هویت، فاش کردن اطلاعات حساس و مکان، امنیت کاربران را به خطر می‌اندازند. کودکان نیز به طور ویژه در معرض تهدیداتی همچون مهاجمان برخط (آنلاین) و آزار و اذیت سایبری قرار دارند. (بهرام‌پور، ۱۳۸۳: ۲۱؛ سعادت سیرت، ۱۳۹۷: ص ۱۱۵؛ ذاکری و رضاپور، ۱۳۹۷: ۹۵-۹۶)

۱.۵ تهدیدات مدرن

در تهدیدهای مدرن امنیت کاربر را به خطر می‌اندازند که از این تهدیدات می‌توان به موارد زیر اشاره نمود (فایر، گلدشمیت، الوویچی[۴]، ۲۰۱۴: ۲۰۲۱).

۱.۱.۵ Clickjacking

نوعی از حملات هکرها است که با کلیک‌کردن کاربر بر روی یک عنصر وبگاه، عنصر دیگری که به‌صورت نامرئی و مخفی است اجرا می‌شود. این حمله باعث می‌شود که کاربران به‌صورت ناخواسته نرم‌افزارهای مخرب را دانلود کنند، به صفحات جعلی هدایت شوند و اطلاعاتشان به سرقت برود (جثاوا، گوردان و رائو، پراتاپ، ۲۰۲۴: ۷).

۲.۱.۵ تشخیص چهره

بسیاری از کاربران شبکه‌های اجتماعی تصاویر خود را در پلتفرم‌هایی مانند فیس‌بوک آپلود می‌کنند که برخی از این تصاویر به طور عمومی در دسترس هستند. این تصاویر می‌توانند برای ساخت پایگاه‌های داده بیومتریک

[۱] Spammers
[۲] بدافزار نرم‌افزار مخربی است که برای ایجاد اختلال در عملکرد رایانه به‌منظور جمع‌آوری اطلاعات کاربری و دسترسی به اطلاعات خصوصی وی توسعه‌یافته است. بدافزار در شبکه‌های اجتماعی از ساختار شبکه اجتماعی آن‌لاین (OSN) برای انتشار خود در بین کاربران و دوستان آن‌ها در شبکه استفاده می کند.
[۳] حملات فیشینگ نوعی مهندسی اجتماعی برای به‌دست‌آوردن اطلاعات حساس و خصوصی کاربر با جعل هویت شخص ثالث قابل‌اعتماد است.
[4] Fire, M., R. Goldschmidt, and Y. Elovici

استفاده شوند و مهاجمان می‌توانند با تحلیل آن‌ها و استفاده از فناوری تشخیص چهره[5] اطلاعات شخصی کاربران را بدون رضایت آن‌ها شناسایی کنند (فایر، گلدشمیت، الوویچی، ۲۰۱۴: ۲۰۲۳).

۳.۱.۵ پروفایل‌های جعلی

پروفایل‌های جعلی[6] که رفتارهای انسانی را در شبکه‌های اجتماعی شبیه‌سازی می‌کنند، برای جمع‌آوری اطلاعات شخصی کاربران، آغاز حملات سایبری (حملات سیبیل[7] یا حملات چند هویتی) (دوکور[8]، جان، ۲۰۰۲: ۲۵۱–۲۶۰)، انتشار هرزنامه (گائو[9] و همکاران، ۲۰۱۰: ۳۵–۴۷) یا حتی تحریف آمار شبکه‌های اجتماعی آنلاین (استرینگینی[10] و همکاران، ۲۰۱۳: ۱۶۳–۱۷۶) استفاده می‌شوند.

۴.۱.۵ حملات شبیه‌سازی هویت

با استفاده از حملات شبیه‌سازی هویت[11]، مهاجمان حضور آنلاین کاربر را در همان شبکه یا در شبکه‌های مختلف شبیه‌سازی می‌کنند تا دوستان کاربر شبیه‌سازی‌شده را فریب دهند تا با پروفایل شبیه‌سازی‌شده تعامل برقرار کنند. مهاجم می‌تواند از این اعتماد برای جمع‌آوری اطلاعات شخصی دوستان کاربر یا انجام انواع مختلف کلاهبرداری آنلاین استفاده کند. نمونه‌ای از حمله شبیه‌سازی هویت اخیراً با ارشدترین فرمانده ناتو، دریاسالار جیمز استاوریدیس[12] رخ داد. جزئیات پروفایل او شبیه‌سازی شد و سپس برای جمع‌آوری اطلاعات در مورد مقامات وزارت دفاع و سایر مقامات دولتی با فریب‌دادن آن‌ها به دوست‌شدن با پروفایل تازه شبیه‌سازی شده فیس‌بوک استفاده شد (لویس[13]، جیسون؛ ۲۰۱۲: ۱۰). حملات شبیه‌سازی هویت از فن‌هایی مانند ردیابی کوکی‌ها، توپولوژی شبکه و عضویت در گروه کاربر برای کشف هویت واقعی کاربر استفاده می‌کنند.

۵.۱.۵ افشای مکان

با افزایش استفاده از دستگاه‌های تلفن همراه هوشمند، بسیاری از افراد از شبکه‌های اجتماعی آنلاین برای به اشتراک گذاشتن اطلاعات حساس مکانی خود استفاده می‌کنند. تحقیقات (همفریس، گیل، و کریشنا مورتی، ۱–۲۹) نشان داده‌اند که درصد قابل‌توجهی از توییت‌ها شامل زمان و مکان کاربران است، و حتی چارچوب‌هایی برای تخمین دقیق مکان کاربر از محتوای توییت‌ها ارائه شده است. نمونه‌ای از این تهدیدات، وبگاه Pleaserobme.com است که اطلاعات مکانی کاربران را افشا[14] می‌کند، مانند تصویری که مجری

[5] Face Recognition
[6] Fake Profiles
[7] sybil
[8] Douceur
[9] Gao
[10] Stringhini
[11] Identity Clone Attacks
[12] Admiral James Stavridis
[13] Lewis
[14] Location Leakage

برنامه MythBusters به اشتراک گذاشت و محل دقیق خانه‌اش مشخص شد.

۲.۵ حملات سنتی

برخی از حملات با استفاده از فن‌های سنتی حمله که از زمان پیدایش اینترنت وجود داشته‌اند، اتفاق می‌افتند. فیشینگ و بدافزار از جمله حملات سنتی شناخته‌شده‌ای هستند که برای سرقت اطلاعات شخصی کاربران استفاده می‌شوند. با به‌دست‌آوردن اطلاعات حساس مانند شناسه کاربری، رمز عبور، شماره‌تلفن همراه، جزئیات حساب بانکی و غیره، یک مهاجم می‌تواند انواع مختلفی از جرایم را در محیط شبکه‌های اجتماعی آنلاین (OSN) مرتکب شود. اگرچه محققان پیش‌تر به این حملات پرداخته‌اند، اما با توسعه OSN ها، این حملات می‌توانند نسبت به گذشته آسان‌تر و سریع‌تر انتشار یابند. برخی از این تهدیدات جدی در اینجا موردبحث قرار گرفته‌اند.

۱.۲.۵ فیشینگ

فیشینگ نوعی حمله جعلی است که در آن مهاجم با استفاده از هویت جعلی یا شخص ثالث، اطلاعات شخصی کاربر را به دست می‌آورد. در حملات فیشینگ در شبکه‌های اجتماعی آنلاین (OSN)، مهاجمان اطلاعات کاربران را جمع‌آوری کرده و قربانیان را از میان آنها انتخاب می‌کنند. آنها یک وبگاه جعلی ایجاد می‌کنند که شبیه به وبگاه اصلی به نظر می‌رسد و سپس پیامی جعلی حاوی لینک فیشینگ ارسال کرده یا آن لینک را بر روی صفحه کاربران قربانی منتشر می‌کنند. وقتی کاربر روی آن لینک کلیک می‌کند، وبگاه فیشینگ باز می‌شود و کاربر با این تصور که وبگاه اصلی است، اطلاعات خود را وارد می‌کند. مهاجمان از این طریق اطلاعات شخصی کاربر قربانی را سرقت می‌کنند (جین[15] و همکاران، ۲۰۲۱: ۲۱۶۳).

۲.۲.۵ بدافزار

بدافزار شامل کدهای مخرب مانند ویروس‌های رایانه‌ای و کرم‌ها است. باتوجه‌به اینکه شبکه‌های اجتماعی آنلاین (OSN) ساختاری شبیه به گراف دارند که در آن کاربران به‌عنوان گره‌ها و ارتباطات به‌عنوان پیوندهای بین آنها عمل می‌کنند، بدافزار می‌تواند به‌راحتی از طریق این پیوندها منتشر شود. بیشتر شبکه‌های اجتماعی آنلاین مکانیزم مناسبی برای تشخیص اینکه آیا یک برنامه یا لینک مخرب است یا خیر ندارند. هنگامی که کاربر بر روی چنین لینک یا برنامه‌ای کلیک کرده یا آن را باز می‌کند، بدافزار منتشر شده و اطلاعات محرمانه کاربر را از رایانه یا تلفن همراه وی سرقت می‌کند (بهاچاریه[16] و همکاران،۲۰۲۳، ۱۲).

علاوه بر این، هرزنامه‌ها نیز به‌عنوان تهدید امنیتی و یکی دیگر از حملات سنتی، می‌توانند منجر به مزاحمت برای کاربران و سرقت اطلاعات شخصی شوند.

[15] Jain
[16] Bhattacharya

۳.۵ تهدیدات ترکیبی

مهاجمان در شبکه‌های اجتماعی آنلاین با ترکیب تهدیدهای کلاسیک مانند فیشینگ و حملات مدرن مانند کلیک‌جکینگ، حملات پیچیده‌ای ایجاد می‌کنند، مانند دسترسی به رمز عبور کاربر و انتشار ویروس در بین دوستان کاربر یا با استفاده از پروفایل‌های جعلی، اطلاعات شخصی دوستان او را جمع‌آوری کرده و از آن‌ها برای ارسال ایمیل‌های مخرب حاوی ویروس استفاده می‌کنند.

۴.۵ تهدیداتی که کودکان را هدف قرار می‌دهد

کودکان، چه خردسالان و چه نوجوانان، مطمئناً تهدیدات کلاسیک و مدرن را که در بخش قبلی توضیح داده شد، تجربه می‌کنند، اما تهدیداتی نیز وجود دارد که عمداً و به طور خاص کاربران جوان‌تر شبکه اجتماعی آنلاین را هدف قرار می‌دهند.

۱.۴.۵ مهاجمان آنلاین

بزرگ‌ترین نگرانی در مورد ایمنی اطلاعات شخصی کودکان مربوط به پدوفیل‌های اینترنتی[۱۷] یا مهاجمان آنلاین[۱۸] است. محققان (لیوینگستون و هادون[۱۹]، ۲۰۰۹ در یونیسف، ۲۰۱۱: ۱) سه آسیب مربوط به فعالیت مهاجمان آنلاین شناسایی کردند: آسیب ناشی از محتوا (مانند مواجهه با پورنوگرافی)، آسیب ناشی از تماس (مانند برقراری ارتباط با افراد متجاوز)، و آسیب ناشی از رفتار (کودکی که به طور فعال در رفتارهای خطرناک مشارکت می‌کند). این رفتارها شامل بهره‌کشی جنسی و تولید پورنوگرافی کودکان است.

۵.۵ آزار و اذیت سایبری

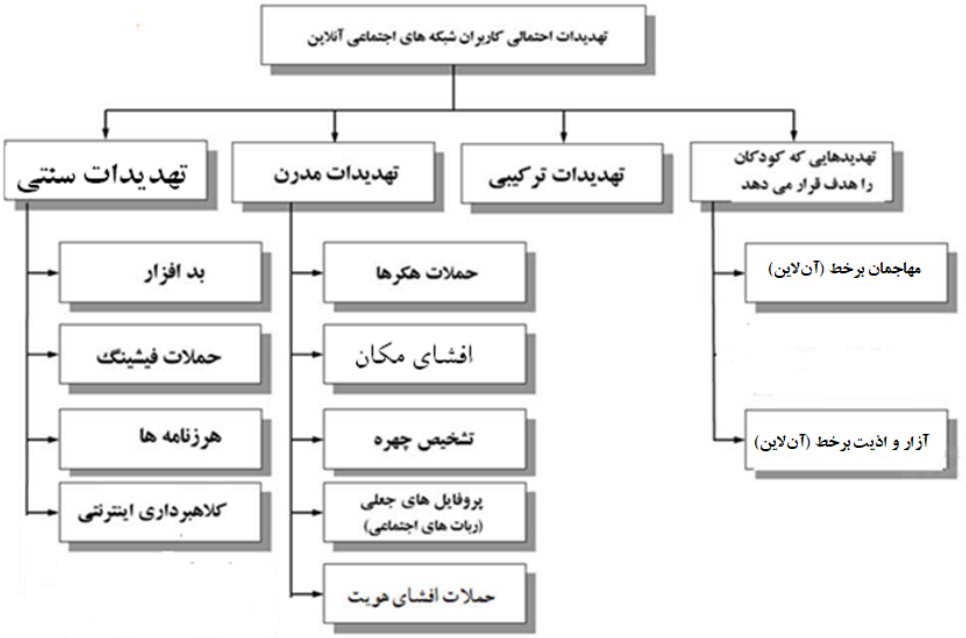
آزار و اذیت سایبری[۲۰] نوعی تهدید سایبری است که از بسترهای ارتباطی دیجیتال مانند ایمیل و شبکه‌های اجتماعی برای تهدید، ارسال پیام‌های آزاردهنده، و انتشار تصاویر شرم‌آور قربانی استفاده می‌کند. این پدیده رایج در فضای آنلاین امکان انتشار شایعات بی‌رحمانه و تصاویر خجالت‌آور را برای مهاجمان فراهم می‌سازد (فایر، گلدشمیت و الوویچی[۲۱]، ۲۰۱۴: ۲۰۲۵).

۶ راه‌کارهایی برای تهدیدات مختلف

محققان سعی کرده‌اند راه‌حل‌های مختلفی برای تهدیدات فوق در رسانه‌های اجتماعی پیدا کنند. آن‌ها چندین روش برای مقابله با این تهدیدات پیشنهاد کرده‌اند:

---

[17] Internet pedophiles
[18] Online Predators
میل جنسی به اطفال که در کشورمان از عبارت بچه‌باز یا کودک‌آزاری استفاده می‌کنند (موسوی؛ (۱۴۰۱). ص ۶۹)
[19] Livingstone and L Haddon
[20] Cyberbullying
[21] Fire, M., R. Goldschmidt, and Y. Elovici



شکل ۱: تهدیدات احتمالی کاربران شبکه های اجتماعی آنلاین

- **تنظیمات امنیتی و حریم خصوصی:** شبکه‌های اجتماعی تنظیماتی ارائه می‌دهند که به کاربران امکان می‌دهد دسترسی به اطلاعات شخصی خود را واپایش کنند و از دیده‌شدن توسط افراد یا برنامه‌های ناخواسته جلوگیری کنند (بلستروم[۲۲] و دیگران، ۲۰۱۶: ۵۴۸-۵۶۷).
- **گزارش‌دهی سریع و پشتیبانی:** کاربران باید بتوانند محتوای نامناسب و نقض‌های امنیتی را به‌سرعت گزارش دهند و شبکه‌ها باید با سیستم‌های پشتیبانی قدرتمند این گزارش‌ها را پیگیری کنند (هنری و بوسمن[۲۳]، ۲۰۱۴: ۴۳-۶۲).
- **تأیید هویت دومرحله‌ای:** این روش امنیت حساب‌ها را افزایش می‌دهد و نیازمند ورود کد امنیتی در کنار رمز عبور است.
- **آموزش کاربران:** افزایش آگاهی کاربران در مورد تهدیدات سایبری و مدیریت اطلاعات شخصی از راهکارهای مؤثر است.
- **استفاده از الگوریتم‌های پیشرفته:** شبکه‌های اجتماعی از هوش مصنوعی و یادگیری ماشین برای شناسایی فعالیت‌های مشکوک و جلوگیری از انتشار اطلاعات نادرست استفاده می‌کنند.

[22] Bellström
[23] Henry and L. Bosman

- **نظارت و قوانین دولتی:** قوانین دولتی باید به محافظت از حریم خصوصی کاربران کمک کنند، مشابه مقررات GDPR در اروپا.
- **پیشگیری از حساب‌های جعلی:** احراز هویت بیومتریک می‌تواند از ایجاد حساب‌های جعلی جلوگیری کند.
- **پشتیبانی از رمزنگاری اطلاعات:** اطلاعات کاربران باید با رمزنگاری انتقال داده شود تا در صورت دسترسی غیرمجاز محافظت شود.
- **فیلترکردن محتوای آسیب‌زا:** شبکه‌ها می‌توانند از فیلترهای خودکار برای جلوگیری از انتشار محتوای مضر استفاده کنند.
- **همکاری بین‌المللی:** تبادل اطلاعات و همکاری بین کشورها می‌تواند در مبارزه با جرایم سایبری مؤثر باشد.

۷ نتیجه‌گیری

این پژوهش نشان داد که شبکه‌های اجتماعی مجازی به‌عنوان ابزارهای تأثیرگذار در زندگی روزمره کاربران، فرصت‌های بی‌نظیری برای ارتباطات و تبادل اطلاعات فراهم می‌آورند. بااین‌حال، چالش‌های جدی از جمله تهدیدات امنیتی و نقض حریم خصوصی برای کاربران به وجود آوردند. براین‌اساس، توجه به راهکارهای مؤثر در مدیریت این چالش‌ها از جمله تنظیمات امنیتی و افزایش آگاهی کاربران ضروری است. این مقاله به‌عنوان یک منبع علمی، به درک بهتر تهدیدات و فرصت‌های موجود در فضای مجازی کمک کرده و برای پژوهش‌های آینده در زمینه‌های مرتبط و به‌ویژه تأثیرات اجتماعی و فرهنگی این شبکه‌ها پیشنهادهایی ارائه می‌دهد.

مراجع

[۱] بهرامپور، شعبانعلی (۱۳۸۳). انسجام اجتماعی در جامعه اطلاعاتی: نیم‌نگاهی به وضعیت ایران، سمینار ایران و جامعه اطلاعاتی.

[۲] ذاکری، محمد مهدی و رضاپور، رویا (۱۳۹۷). چالش‌ها و تهدیدها نظام خانواده در بستر شبکه‌های اجتماعی مجازی، تهران: انتشارات آکادمیک.

[۳] زارعی، علی (۱۳۹۶). فرصت‌های آموزشی در شبکه‌های مجازی و رسانه‌های اجتماعی، چاپ اول، مؤسسه فرهنگی هنری دیباگران تهران.

[۴] سعادت سیرت، ناهید (۱۳۹۷). شبکه‌های اجتماعی مجازی، فرصت‌ها وپیامدها، همدان، سپهر دانش.

[۵] موسوی، اسماعیل (۱۴۰۱). «حمایت کیفری از اطفال بزه‌دیده جنسی در حقوق کیفری ایران و فرانسه»، قم: تخت سلیمان؛ چاپ اول.

[۶] نوکاریزی، محسن (۱۳۹۴). آشنایی با اطلاعات و ارتباطات. چاپ دوم، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).

[7] Ali, S., et al., Privacy and security issues in online social networks. Future Internet, 2018. 10(12): p. 114.

[8] Bellström, P., et al., Facebook usage in a local government: A content analysis of page owner posts and user posts. Transforming Government: People, Process and Policy, 2016. 10(4): p. 548-567.

[9] Bhattacharya, M., et al., A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges. Security and Privacy, 2023. 6(1): p. e275.

[10] Boyd, D.M. and N.B. Ellison, Social network sites: Definition, history, and scholarship. Journal of computer-mediated Communication, 2007. 13(1): p. 210-230.

[11] Buhl, H.U., Online-Communitys–der Weg zur Gruppenintelligenz oder zur Gruppenignoranz und kollektiven Verdummung? Wirtschaftsinformatik, 2008. 50: p. 81-84.

[12] Douceur, J.R. The sybil attack. in International workshop on peer-to-peer systems. 2002. Springer.

[13] Ferrag, M.A., L. Maglaras, and A. Ahmim, Privacy-preserving schemes for ad hoc social networks: A survey. IEEE Communications Surveys & Tutorials, 2017. 19(4): p. 3015-3045.

[14] Fire, M., R. Goldschmidt, and Y. Elovici, Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials, 2014. 16(4): p. 2019-2036.

[15] Gao, H., et al. Detecting and characterizing social spam campaigns. in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. 2010.

[16] Guo, Z., et al., Online social deception and its countermeasures: A survey. Ieee Access, 2020. 9: p. 1770-1806.

[17] Henry, R. and L. Bosman, Strategic management and social media: An empirical analysis of electronic social capital and online fundraising, in Social media in strategic management. 2014, Emerald Group Publishing Limited. p. 43-62.

[18] Humphreys, L., P. Gill, and B. Krishnamurthy. How much is too much? Privacy issues on Twitter. in Conference of international communication association, singapore. 2010.

[19] Jain, A.K., S.R. Sahoo, and J. Kaubiyal, Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 2021. 7(5): p. 2157-2177.

[20] Jethava, G. and U.P. Rao, Exploring security and trust mechanisms in online social networks: An extensive review. Computers & Security, 2024: p. 103790.

[21] Kayes, I. and A. Iamnitchi, Privacy and security in online social networks: A survey. Online Social Networks and Media, 2017. 3: p. 1-21.

[22] Lewis, "How spies used facebook to steal NATO chiefs' details," The Telegraph, London, U.K., Mar. 2012. [Online]. Available: http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs details.html.

[23] Lewis, J., How spies used facebook to steal nato chief's details. The Telegraph, 2012. 10.

[24] Murphy, K., Web photos that reveal secrets, like where you live. The New York Times, 2010. 11.

[25] Peng, S., et al., Influence analysis in social networks: A survey. Journal of Network and Computer Applications, 2018. 106: p. 17-32.

[26] Ramalingam, D. and V. Chinnaiah, Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, 2018. 65: p. 165-177.

[27] Rathore, S., et al., Social network security: Issues, challenges, threats, and solutions. Information sciences, 2017. 421: p. 43-69.

[28] Sahoo, S.R. and B.B. Gupta, Classification of various attacks and their defence mechanism in online social networks: a survey. Enterprise Information Systems, 2019. 13(6): p. 832-864.

[29] Sarmah, U., D. Bhattacharyya, and J.K. Kalita, A survey of detection methods for XSS attacks. Journal of Network and Computer Applications, 2018. 118: p. 113-143.

[30] Stringhini, G., et al. Follow the green: growth and dynamics in twitter follower markets. in Proceedings of the 2013 conference on Internet measurement conference. 2013.

[31] Taylor, C., Startup claims 80% of its facebook ad clicks are coming from bots. 2012, Technical report, 2012. available at http://techcrunch.com/2012/07/30.

[32] Unicef, Child safety online: Global challenges and strategies. 2011, Innocenti Publications.