# یک مطالعه جامع در مورد حفظ حریم شخصی و امنیت در رسانه های اجتماعی


## چکیده

شبکه های اجتماعی تبدیل به بخشی از زندگی انسانی شده است.از ابتدا با اشتراک گذاری متن، تصاویر، پیغام شروع شده بود و اخیرا به اشتراک گذاری آخرین اخبار،تصاویر مرتبط با اخبار در حوره رسانه ها،مقالات پرسشی،تکالیف درسی ، و کارگاه های آموزشی در حوزه آموزش و پرورش، بررسی های آنلاین،بازاریابی،و هدف قرار دادن مشتریانی در حوزه کسب و کار، و جوک،موسیقی،و ویدئو در حوزه سرگرمی می پردازد.به دلیل اینکه توسط خوانندگان اینترنتی مورد استفاده قرار می گیرد،برای همین ما ممکن است ما از رسانه های شبکه های اجتماعی به عنوان فرهنگ فعلی اینترنت یاد کنیم.در حالیکه ما از به اشتراک گذاری اطلاعات در رسانه های اجتماعی لذت می بریم،با این حال همچنان بحث امنیت و حفظ حریم شخصی یک بحث بزرگ در این زمینه است.اطلاعات کاربرانی که تمایل به فاش شدن آن اطلاعات ندارند باید به صورت خصوصی نگهداری شود.



**کلمات کلیدی:** رسانه های اجتماعی،حریم شخصی،اجرای سیاست،امنیت


## 1. مقدمه

در چهارچوب بزرگتری از داده کاوی، یک اندازه گیری قابل توجهی از تجزیه و تحلیل تولید کننده ها صورت گرفته است تا بتوان بر اساس آن به سوابقی پیشرفته از رفتار انسانی بین فردی را در سازمان ها و بدون نقض حریم شخصی کاربران داشت.بنابراین،اطلاعات باید اطلاعات به شیوه ای در دسترس باشند که در آن حفظ حریم شخصی به شکلی

کحافظت شده و با حفاظتی بسیار مورد بررسی قرار بگیرد.از طرفی دیگر، سوء ظن نسبت به کسانی که تمایل به تجاوز به این حریم و دسترسی به اطلاعات شما را دارند نیز باید در نظر گرفت و نباید به انها اعتماد کرد، زیرا ممکن است هدف اصلی آنها استفاده از تمامی اطلاعات شما باشید، برای همین باید شناخت و شناسایی مواردی که حساس است، برای این جمع آوری ها لازم می باشد.با توجه به نمونه خاصی از سازمان های بین فردی،پایه ترین اندازه گیری که می توان برای پایدار شدن کیفیت حریم شخصی افراد انجام داد را به وسیله بیان وابستگی ها می توان نشان داد.

با توجه به نویسندگان [3]،که پیشنهاد داده بودند هر گونه از بررسی در مورد تعداد مشتریانی که تمایلاتشان را بیان کرده اند، سبب خنثی شدن موارد امنیتی که برای حفاظت از خطر آنها فراهم شده بود می شود و همچنین این موارد نیازمند بررسی حیاتی است.پیشنهاد این نویسندگان این است که ارتباطی آماده برای سازمان های بین فردی و پروفایل کاربران ساکن در آن آماده باشد، اما به مشتریان اجازه شریک شدن در برآورد برخی از اموال تضمین شده با استفاده از اعتبار خودشان را بدهیم، اما هر بار مقداری از بیان اعتبار آنها برای این آشکار سازی لازم می باشد.از دید چشم انداز حریم شخصی [1] ، موضوع حریم شخصی تحت بررسی می باشد و برای اطمینان از اهمیت اساسی آن گروهی علمی خاصی مامور شده اند که مراقب آن باشند.برای اطمینان از حفظ حریم شخصی مشتریان شناخت ویژگی های آنها انجام می شود،و نه آسیب پذیری بر اساس بینام سازی رخ می دهد.بنابراین با توجه به این حقیقت که تنها از  یک دید تخصصی جواب ما بیشتر نزدیک به حفظ حریم شخصی تا محافظت به خصوص در طولانی مدت است،حفظ اطلاعات شخصی مشتریان تضمین شده است.

علاوه بر این، بررسی های ناشناخته ای که مرتبط با ویژگی های مختلفی از جمعیت عمومی است که تمایل به  ایجاد ارتباطی با یکدیگر و  بی خطر برای حریم شخصی کاربران دارند، در سایه این حقیقت که هیچ راه حل واقعی ای برای ارتباط داده ها به یک کاربر خاص وجود ندارد صورت گرفته است.علاوه بر این، پیش نیازهایی که در بالا مطرح شده اند سبب فراهم شدن آشکارسازی مخصوصی می شود و روشهایی که ذره ای در آن مسئولیت پذیری نیز وجود دارد، هنوز از جمله راه هایی فوری برای استفاده در جهت مقابله با مورد ما نمی باشد زیرا ثابت نمی باشد و از آنجایی که این مکانیزم ها به افراد غیر خودی اجازه دنبال کردن کاربرها را می دهد،پس به دنبال خود سبب نقض گمنامی

می شود.و این مشکلی که در این مسیر وجود دارد بی ارزش نیست.راه حل کلیدی بستگی به یک رمزنگاری قرار دادی دارد که در آن حریم خصوصی در درجه اول از نظر غیر قابل اجرا بودن لگاریتم هایی گسسته و قدرت امضایی که تا حدودی توسط افراد قابل مشاهده نیست مورد بررسی قرار می گیرد[7].در حقیقت،ما می توانیم فیسبوک را به این شکل در نظر بگیریم که تنها یک رابطه مثبت آنلاین که حول کاربران شبکه احتماعی وجود دارد نیست.حفظ حریم شخصی کاربران ثبت نام شده و جلوگیری از وقوع هر گونه انحرافی از سیاست های داده شده که به نوبه خود می توانند سبب ویرانی جدی حقوق اصلی جامعه می شود را می توان به عنوان نقش اصلی گردانندگان فیسبوک دانست.در رسانه های اجتماعی،برخی از داده های شخصی توسط کاربران چه به صورت آگاهانه و چه به صورت ندانسته به اشتراک گذاشته می شود.برخی اوقات، این اطلاعات خصوصی توسط خود کاربران به صورت آگاهانه به اشتراک گذاشته می شود و در ازای آن برخی از مزایا برای این کاربران فراهم می شود.در طی خدمات شبکه های اجتماعی که مبتنی بر مکان هستند ( که به اختصار LBSNS نامیده می شوند)مانند FireEagle ، Google Latitude ، Nearby و ... می باشد.

## 2. تهدیدات احتمالی و خطرات حریم شخصی در سایت های شبکه های اجتماعی

طبق نظریه آنالیز حریم شخصی،عوامل تعیین کننده بر روی مزایا و خطرات آزادی نظارت می کنند که بر روی انتخاب یک کاربر برای آشکارسازی میزان اعتبار معین وی تاثیر می گذارد.علاوه بر این اینگونه پیشنهاد شده است که افرادی که به ندرت مشتاق به مخفی کردن حریم خصوصی خود هستند نیز در سطح بالایی از خطر قرار دارند. با استفاده از سایت های شبکه های اجتماعی [4]، مردم خودشان را در برابر انواع خطراتی که سبب از بین رفتن حریم خصوصی آنها می شود باز نگه می دارند.بارها شاهد بودیم که اگر اطلاعات شخصی به شکلی منطقی و دقیق مورد استفاده قرار نگیرد حریم شخصی مورد حمله قرار می گیرد. سازندگان پیشنهاد داده اند که همواره به مواردی که مرتبط با حفاظت اطلاعات خودتان هستند پایبند باشید زیرا در غیر این صورت حملاتی از این طریق رخ می دهد که علت آن از بین رفتن حریم خصوصی و یا تانوانی استراتژی های ناتوان کننده می باشد.افزون بر آن، آنها تخمین زده

اند که نفوذ به حریم شخصی می تواند در هنگام پر کردن اطلاعات اختیاری برای یک طرحی مثل دیدار در تعطیلی های مختلف و بدون موافقت صاحب اطلاعات رخ بدهند. با این وجود، اگر استراتژی های مناسب اطلاعاتی به همراه استفاده درست مردم از اطلاعات خودشان و کنترل این دست از اطلاعات رخ دهد،نگرانی هایی که بابت حفظ حریم شخصی وجود دارد را می توان برطرف کرد. به صورت مقایسه ای می توان اینطور گفت که،که این فرضیه بیان می کند که افشاء اطاعات یک ابزار خاصی است که به کاربران اجازه کنترل استفاده در آن را با توجه به اهداف خود، یادگیری و ذهنیت نسبت به حفاظت می دهد.در محدوده اتصلات بین فردی در جامعه اجتماعی آنلاین، چنین حد مقرراتی از طریق تنظیماتی در داخل بخش تنظیمات حریم خصوصی [8] انجام می شود.این تنظیمات امنیتی سبب بهبود ظرفیت کاربران در افشای اطلاعات و علاوه بر آن سبب هموار تر شدن مسیری می باشد که در آن دادن اطلاعات تنظیمات با توجه به نیاز است.

### 2.1 نقض افشای اطلاعات

اصلی ترین نگرانی که در مورد شکست حریم خصوصی وجود دارد این است که اعتبار کاربر شبیه به یک قرارداد اجتماعی است که در آن کاربر داده های خودش را در مقابل پاداش های مالی و یا غیر مالی معامله می کند.کاملا مشخص است که کاربران قضایی به این نوع از قراردادهای اجتماعی علاقه مند هستند زیرا مزایای آن سبب پیش افتادن آنها از خطرات حال و حتی خطراتی که در آینده ممکن است در معرض آن قرار بگیرند است.پیشنهاد قابل اعتمادی که با این فرضیه مطرح می شود این است که ، مردم با این تصمیم گیری ها بمانند و سبب تجربه بیشترین مزایا و همچنین به حداقل رساندن هزینه ها شوند.و این قضیه اینگونه راه اندازی شده است که از به فاش کردن اطلاعات کاربران بر روی سایت های شبکه های اجتماعی می پردازد. از آنجایی که هدف پیشنهادی مشاهده تاثیرات ذاتی مزایا می باشد، افشاء به دو بخش ساختاری تقسیم بندی می شود:یک قسمت به اندازه گیری میزان آمادگی کاربران پیش از دریافت پاداش برای افشاء می باشد در حالیکه کاربران را به سمت افشاء اطلاعات خود برای دریافت پاداش سوق می دهد.شرایط غیر ظاهری باطنی-بیرونی طبق [2] می باشد.

در کارهای اولیه نشان داده شد که هدف از افشاء می تواند اندازه گیری میزان توسعه خاصی به صورت آزاد باشد.

## 3. متدولوژی پیشنهادی برای مشکلات مرتبط با حریم شخصی در سایت های رسانه های اجتماعی

هدف اصلی این مطالعه اتصال یک سیستم کمی به یک هدف نهایی مشخص برای بررسی اطلاعات اجتماعی دروغین از کاربرهای بالقوه و بدست آوردن جزئیات مورد نیاز مانند داده های دموگرافیک ( جمعیت شناسی) ، داده های موقت، پروفایل های کاربران و سایر مواردی این چنینی از پاسخ دهنگدان است.برای تقویت این روند، ما یک بررسی بر روی سیستمی که به طور کامل در بین بیش از 200 نفر از کاربران رسانه های اجتماعی انجام می شود که توسط تست های استراتژی های غیر احتمالی بر روی مردم انجام خواهد گرفت.تست اسپیرال (مارپیچ) و پاسخ های ناشی از آن به تحلیل گران اجازه اندازه گیری معیاری در مورد سازمان های پیوندی بین فردی می دهد که در حال حاضر آنها از مردم برای حمایت از شبکه اجتماعی جوامع حال حاضر التماس می کنند.بنابراین،این مطالعه جامع بر روی نگرانی های اصلی شبکه های اجتماعی بیشتر تمرکز کرده است و امیدوار است که بتوان خروج از حریم شخصی را به صورت موثرتری مورد شناسایی قرار دهیم.ما برخی از نگرانی هایی که در مورد حریم شخصی کاربران اجتماعی وجود داشت که آنها باید پیش از استفاده از سایت های شبکه های اجتماعی مسئولیت آن را بر عهده بگیرند و تنظیمات حریم شخصی آن را در داخل تنظیمات سایت به منظور جلوگیری از هرگونه نقضی در حریم شخصی خودشان باید انجام دهند.

### 3.1 پیش بینی رفتار کاربران رسانه های اجتماعی

این مطالعه با هدف کشف حریم شخصی و حریم شخصی در میان سایت های شبکه های اجتماعی که در میان سایر شبکه های محلی  و توسط مشتریان به رسمیت شناخته می شود انجام شده است[6]. یک نمونه مطالعاتی شامل 250 مورد برای این فرضیه و از نقاط متمایزی از جهان انتخاب شده بودند.از طرفی دیگر تقریبا 72 نفر از پاسخ دهندگان دارای سنی بین 20 الی 35 سال بودند.که در آن ممکن است، تعداد تجمع سنی بین 28 الی 41 عملا

19% بوده است در حالیکه تفاوت تجمعی 50 یا بیشتر در حدود 0 بوده است.سطح آموزشی این افراد تاثیر به سزایی داشته باشد ، 58٪ این افراد دارای مدرک لیسانس و فارغ التحصیل بودند که حدود 21 ٪ از این جامعه بودند. سالهای استفاده از اینترنت در این سازمان مشترک بین فردی بر اساس افرادی که در حال استفاده از وب برای حدود 10 سال هستند به 56٪ می رسد و در رویداد هایی که ماهیت اتصال آن با استفاده از SN طبیعی بوده است دارای شاخص 51٪ برای سازمان های خوب است و برای سازمانهایی که به شدت شناخته شده هستند این مقدار 49٪ است.سپس دوباره در 90٪ از این جامعه مطالعاتی مردم از فیسبوک استفاده می کنند و 36 ٪ از اسلام تگ استفاده می کنند و 62٪ از توییتر استفاده می کنند برای همین استفاده از مدل حفاظتی فیسبوک برای ما آزادی عمل بیشتری را به همراه خواهد داشت.

### 3.2 اشکالها و نگرانی های حفظ حریم شخصی

همانطور که در جدول 1 به تصویر کشیده شده است،هنگامی که برخی از اطلاعات را در مورد حفظ حریم شخصی دریافت کردیم و اینکه مردم تا چقدر با حفاظت از آن اطلاعات از نظر شرایط نگهداری آشنا هستند،52 ٪ با این عناصر نگهداری تا حد متوسط آشنا بودند و طراحی مجدد بخش حفاظت رسانه های اجتماعی نشان داده است که در حدود 87٪ تنها با این محافظت در حد اینکه بخش خاصی از پروفایل خودشان می باشد آشنایی دارند [2] ، در مورد تغییرات این محافظت 43٪ از افراد اغلب تنظیمات حریم شخصی خودشان را تغییر می دهند به خصوص زمانی که اتفاقی افتاده باشد و 47٪ هر از گاهی این تنظیمات را تغییر می دهند و همین روند برای تنظیمات رکورد ها و حریم شخصی آنها نیز صدق می کند.

در جدول 1 در زیر، ما مکانسیم های مختلفی را برای حریم شخصی مورد شناسایی قرار دادیم که این مکانیسم ها توسط سایت های رسانه های اجتماعی به کاربران پیشنهاد می شود تا مطابق آن تنظیمات را در مورد حریم شخصی فعالیت های خود انجام دهند.در این بررسی صورت گرفته یک دامنه گسترده ای از تبعیضات در رسانه های اجتماعی و مجموعه هایی که آنها تحت عنوان سیاست های حفظ حریم شخصی به کاربران خود ارائه می دهد وجود دارد که

در اینجا مورد بررسی قرار گرفته است، و تا حد زیادی به آن اشاره شده است که بسیاری از کاربران سایت های رسانه های اجتماعی زیاد به حفظ حریم خصوصی خودشان اهمیت نمی دهند و معمولا جزئیات امنیتی آن را به صورت پیش فرض و طبق همان چیزی که ایجاد شده است حفظ می کنند.

جدول 1 نگرانی های مرتبط با حریم شخصی در سایت های رسانه های اجتماعی و مقایسه آنها با یکدیگر

| گوگل پلاس | لینکدین | توییتر | فیسبوک | گزینه های حریم خصوصی |
|---|---|---|---|---|
| خیر | خیر | خیر | بله | محدود کردن دید از کاربران فعال |
| خیر | بله | بله | بله | تنظیم اینکه دیگران چگونه قادر به یافتن شما باشند |
| بله | خیر | خیر | بله | بلاک کاربران برای تگ کردن شما در عکس ها |
| بله | خیر | خیر | بله | تنظیم هشدار ورودی |
| بله | بله | بله | بله | بلاک اسپم از سوی کاربران |
| بله | بله | خیر | بله | کنترل اینکه چه کسی می تواند به شما پیام دهد |

### 3.3 خطرهای مختلف و احتمالی که ممکن است در سایت های شبکه های اجتماعی رخ بدهد

اصلی ترین نیازمندی سایت های شبکه های اجتماعی بحث مسائل امنیتی و حریم خصوصی است.اما همچنان بسیاری از مرگبارترین نوع حملات در تمامی سایت های شبکه های اجتماعی رخ می دهد و محافظت از کاربران در برابر وظیفه ای چالش برانگیز برای بسیاری از تحلیلگران اجتماعی و توسعه دهندگان بوده است.حملات اساسی امنیتی به سه دسته تقسیم بندی می شوند.

- نقض حریم خصوصی- یافتن ارتباطی بین گره ها و یال ها و شناسایی احتمال وجود رابطه ای بین آنها است.
- حملات منفعل- این دسته از حملات کاملا ناشناس و غیر قابل شناسایی می باشد.
- حملات فعال – گره های جدیدی را شکل دهی می کنند که ذاتا سعی در اتصال به گره های مرتبط و کسب دسترسی به گره های دیگر است.

جدول 2 تصویری واضح از انواع حملاتی که در سایت های رسانه های اجتماعی رخ می دهد را ارائه می دهد و همچنین راه حل هایی احتمالی برای چگونگی مقابله با این حملات به صورت امن را نیز فراهم کرده است[10].

جدول 2 . حملات اصلی، زیر حملات، و سیاست های پیشگیرانه احتمالی

| راه حلی برای رسیدگی به این حملات | زیر حملات | دامنه حملات اصلی [10] |
|---|---|---|
| -استفاده از نرم افزارهای انتی ویروس و آنتی بد افزار | TCP SYN Flood Attack<br>Smurf IP Attack | شبکه های اجتماعی |
| -نصب سیستم هایی مناسب برای تشخیص نفوذ | UDP Flood Attack، پینگ مرگبار، افتادن اشک | حملات زیرساخت |
| -استفاده از آنتی ویروس<br>-به لینک ها،دوستان،نرم افزارها و موارد متصل به ایمیل که ناشناخته هستند اعتماد نکنید.<br>-جلسه ها ،کوکی ها را غیر فعال کنید و اگر هیچ گونه اندازه گیری ناشناخته یا مورد ناشناخته ای وجود داشت Active X را غیر فعال کنید. | جرم ابزارها،جاسوس افزارها،ابزارهای تبلیغاتی و مزاحم، دزدان مرورگری، دانلودکننده ها،نوارهای ابزار | حملات هرزنامه ها |
| -ایمیل ها را با دقت ارزیابی کنید.<br>-منبع داده را مورد اعتبار سنجی قرار دهید.<br>-از پیشنهادات تبلیغاتی آگاه باشید. | Phishing فریبنده( ایمیل ها)، تروجان مبتنی بر Phishing ، کی لاگرها، Phishing مبتنی بر موتورهای جست و جو | حملات Phishing |
| -در مورد یافتن دوست و به اشتراک گذاری اطلاعات با آنها احتیاط کنید.<br>-پروفایل کاربری و داده های به اشتراک گذاشته شده را شناسایی کنید.<br>-سعی کنید که به طول کامل سیاست های مرتبط با داشتن دوست را در سایت های شبکه های اجتماعی را متوجه شوید. | حمله مهندسی اجتماعی | حملات Evil Twin |
| -از رمز عبورهای پیچیده استفاده کنید ، از یک رمز عبور در همه جا استفاده نکنید.<br>-ایمیل ها و یا استاد خود را به درستی تکه تکه کنید. | افتادن سطل آشغال | حملات سرقت هویت |
| -پیام هایی که برای صدمه زدن و یا به عنوان تهدید ارسال شده اند را تایید نکنید.<br>-پیام ها را ذخیره سازی و آرشیو کنید و از آنها به | مزاحمت سایبری | مزاحمت سایبری |

| | | |
|---|---|---|
| عنوان مدارک نگهداری کنید.<br>-تمامی تهدید ها را جدی بگیرید.<br>-اطلاعات شخصی خودتان را با تمامی کاربرها تقسیم نکنید. | | |
| -نیاز به یک سیاست به خوبی تعریف شده از شبکه های اجتماعی وجود دارد.<br>-چک کردن سوابق و اهداف حریم خصوصی.<br>-به درستی از گزینه های مرتبط با تنظیمات حریم شخصی استفاده کنید. | جعل هویت،آزار و اذیت از طریق پیام ها | حملات فیزیکی |

### 3.4 تنظیمات حریم شخصی در سایت های شبکه های اجتماعی

هدف از بررسی سایت های شبکه های اجتماعی تقویت تنظیمات حریم شخصی است. فیسبوک و دیگر شبکه های اجتماعی که دارای محدوده طولانی از ارتباطات هستنمد به عنوان تنظیمات پیش فرض خودشان دارای محافظت محدودی هستند.برای همین کاربران این سایت ها باید به قسمت تنظیمات مراجع کنند تا تنظیمات دلخواه خودشان را جایگزین تنظیمات فعلی سایت کنند.سایت هایی مانند فیسبوک به کاربران خودشان اجازه مخفی کردن اطلاعات شخصی مانند ،داده های مفهومی، ایمیل، شماره تلفن، و وضعیت کسب و کار را می دهد.برای افرادی که تصمیم به ترکیب این موارد دارند، فیسبوک به کاربرانش اجازه صدور دسترسی محدودی به پروفایل افرادی که خودشان را به عنوان "هم نیشن ها" می دانند برای دیدن پروفایل هایشان را می دهد.حتی در چنین سطحی از حریم شخصی نیز باز ممکن هم نشین ها تصویری را از کامپیوتر خودشان بردارند و در جایی دیگر پست کنند. اما همانطور که ممکن است بنظر برسد، در حال حاضر استفاده کنندگان رسانه های اجتماعی معمولا پروفایل خودشان را محدود می کنند. برای مثال، اجازه دهید که نحوه محدود کردن قابلیت مشاهده پروفایل کاربران این سایت ها را توسط سایرین کاربرها را در اینجا توضیح دهیم:

• فیسبوک:تنظیمات حریم شخصی فیسبوک برای کاربران جدید آن به شکل "تنها دوستان" می باشد. باری تنظیم این مورد به قسمت تنظیمات>حریم شخصی> چه کسی می تواند پست های آینده من را ببیند؟ بروید.

• توییتر:تنظیمات>امنیت و حریم شخصی>خریم شخصی در توییتر>محافظت از توییت های من.

• لینکدین:برای تغییر آن باید به قسمت :تنظیمات>اکانت>لینک های کمکی>ویاریش پروفایل عمومی خودتان رجوع کنید.

• گوگل پلاس:برای تغییر این تنظیمات،نام یک دایره را در پایین قسمت "به" را در پایین پست های خودتان پیش از منتشر شدن آن را بنویسید.

فیسبوک به راحتی می تواند بگوید که هیچ گونه غرامتی را در برابر اطلاعات شما با توجه به سیاست های حریم شخصی و اطلاعات به شما نخواهد داد، و اگر مشتری پروفایل خودش را بر روی حالت باز قرار دهد، تمامی داده هایی که درون پروفایل وی موجود است ممکن است توسط اشخاصی مانند مدیر مدرسه و یا توسط پرسشگر های سو استفاده گر مورد بازدید قرار بگیرد.

البته به یاد داشته باشید که اکثر این ارتباطات غیر رسمی از راه دور حتی در صورت ترک این برنامه های کاربردی توسط شما یک مختصر اطلاعات مفیدی از شما را بدون اطلاع شما و به شکلی توطئه آمیز در اختیار دارند.با این حال بیشتر داده ها همچنان به صورت باز در اختیار آنها قرار می کند. این قضیه به نوعی ظالمانه است که حتی کسانی که پروفایل خودشان را در این شبکه های دوربرد اجتماعی به صورت بسته و محدود از لحاظ دسترسی سایر کاربران به پروفایل خودشان در آورده اند، و هیچ گونه داده ای از فعالیت های غیر قانونی با توجه به پست های پروفایل خودشان به جا نگذاشته اند، همچنان باید نگران در دسترس قرار گرفتن داده های خودشان توسط دیگران باشند.

### 4. مدیریت اعتماد و مسائل مرتبط با آن

حفاظت از اطلاعات یک پیش شرط اصلی برای خود افشاگری آنلاین است، با این حال خود قضیه خود افشاگری سبب کاهش حریم شخصی می شود زیرا مشتری های مختلفی به اطلاعات شما به صورت آنلاین دسترسی پیدا می کنند.ارتباط بین این ساختارها به نظر می رسد که تحت تاثیر متغیرهای مهمی قرار دارد، به عنوان مثال، اعتماد و

کنترل[5].اعتماد دارای خصوصیاتی است که به عنوان یک عقیده مطرح می شود که در آن مردم،اجتماعات یا موسسات را برای اعتماد داشتن می توان در نظر گرفت.این مفهوم معمولا در تضاد با محافظت است،زیرا مردم برای اعتماد به فردی دیگر نیاز به دانستن اطلاعات آنها دارند به خصوص اگر هدف نهایی را اعتماد به آنها در نظر بگیریم،بدین ترتیب دارای نتایج مفیدی در مورد خود افشاگری آنلاین نیز وجود دارد.

سپس مجددا، پیشرفت اعتماد در یک دامنه آنلاین بر اساس این حقیقت که دنیای آنلاین شکننده است غیر قابل پیشبینی است.این همان دلیلی است که چندین مطالعه با تمرکز بر روی علت تمایل افراد برای افشا سازی داده های خودشان با وجود اعتماد و حفاظت صورت گرفته است.یک ساختار ضروری که می تواند این رابطه آشفته ذهنی را تحت تاثیر قرار بدهد را کنترل آشکار بر روی داده ها است. برای مثال،بررسی کلمات، و اجزایی که به طور مخصوص ساخته شده اند، و از ارزیابان آماده به طور منظمی برای تعیین کمیت خود افشاگری آنلاین، و از تنظیمات ابزار مونتاژ شده برای ارزیابی مکاتبات شخصی جهت ارزیابی اعتماد آنلاین مورد استفاده قرار می گیرد.

### 4.1 راه اندازی حریم شخصی بر روی سایت های شبکه های اجتماعی

تحقیقات اخیر به بررسی رابطه بین خود افشاگری آنلاین داده های افراد و نگرانی های حریم شخصی و خطرات بالای شناسایی شده که همراه با نابودی محافظت است صورت گرفته است.همچنین به خوبی نشان داده شده است که حریم شخصی یک اصطلاحی است که توصیف آن بسیار سخت می باشد. از لحاظ قانونی، به یکی از طرفینی اشاره می کند که نباید به آن اشاره کرد، با این حال این مزیت را دارد که تعیین کند کدام یک از داده شخصی می تواند آشکار شده باشد، و کدام یک از داده ها،چه زمانی،چگونه،و چه مدل از داده ای را می توان به دیگران نشان داد.پیداکردن اطلاعات خصوصی یکی از ویژگی های پخش کنندگی اینترنت می باشد، که شامل عکس هایی تحقیر آمیز و یا ویژگی هایی هستند که ناشی از حقه های Phishing یا محدودیت کمبود حفاظت می باشند و حاکی از خطرات روانی واقعی هستند.در فیسبوک، تنظیمات به شکلی روان هستند، که دارای انشعابات زیادی با توجه به حق مدیریتی در تنظیمات حریم خصوصی در فیسبوک هستند.معمولا استفاده مشتری ها از این امکانات بسیار محدود

است هم از لحاظ مقیاس و هم از لحاظ اندازه ، و مدیریت محافظت در تنظیمات نیز اغلب گرفتار کننده، بیهوده است و نیاز به ارزیابی های خاصی دارد.در مورد خطرات حفظ حریم شخصی معمولا بسیار کم فکر شده است، در حالیکه مزایای اجتماعی آن در حال ظهور می باشد و غالبا آشکارسازی داده های فردی در این بین دست بالا گرفته می شود. در کنار آن،نقض حریم شخصی آنلاین رایج شده است و به عنوان یک قسمت کار فیسبوک درآمده است، و درخواستهایی که برای داده های فردی وجود دارد سبب ایجاد استرس در مشتری ها نمی شود. این خصوصیات از مدیریت حریم شخصی سبب تاثیر در شرایط نمایی وب در سمت دیدگاه مشتری می شود به طوریکه آنها ممکن است خودشان اقدام به خود آشکارسازی کنند.

## 5. نتیجه گیری

اینگونه مشاهده شد که نگرانی های مرتبط با حریم شخصی در زمینه سایت های شبکه های اجتماعی بسیار ضعیف می باشد همچنین تلاش کاربران برای حفظ حریم شخصی خود در رسانه های اجتماعی بسیار پایین تر از عملیات های امنیتی فراهم شده توسط این سایت ها بوده است.علاوه بر این، بسیاری از کاربران رسانه های اجتماعی دارای کمبودهای فنی در این مورد هستند و با این حال نگرانی نیز در مورد افشا شدن محتوای حریم شخصی خود ندارند.در آماری که مورد بررسی قرار گرفته شده بود،ما بسیاری از این کاستی ها و گاف هایی که از سمت تکنیکی و امنیتی حریم شخصی در مورد سایت های شبکه های اجتماعی وجود داشت را تحت اندازه گیری قرار دادیم .از همین رو ما علت ریشه ای این مشکلات را پیدا کردیم و پیشنهاد تغییراتی برای نگرانی های موجود در مورد حریم شخصی در سایت های شبکه های اجتماعی را نیز ارائه دادیم.اگر ما مجموعه ای درست از سیاست هایی که به خوبی تعریف شده است را برای رسانه های اجتماعی اعمال کنیم ، مانند، یک رمز عبور قوی،آگاهی از نیاز به تغییر کلمه عبور هر چند وقت یکبار،آگاهی از افشای اطلاعات،هدف از آنتی ویروس و یا سایر نرم افزار های مرتبط، و نرم افزار های انحصاری و سایر موارد این چنینی، سبب ایمن شدن شبکه های اجتماعی از حملات و آسیب پذیری های آینده می شود.

## References


1. Basilisa Mvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior, Dec 2014; 4(c):20-34.
2. Joshana Shibchurn, Xiangbin Yan.Information disclosure on social networking sites: An intrinsicęxtrinsic motivation perspective. Computers in Human Behavior. 2015; 44:103-117.
3. Yan Li, Yingjiu Li, Qiang Yan, Robert H. Deng, Privacy leakage analysis in online social Networks, Computers and Security, Mar 2015; 49(c):239-254.
4. Patrick Van Eecke, Maarten Truyens, Privacy and social networks, Computer Law & Security Review ;2010; 26(5):535-546.
5. Benson Vladlena, George Saridakis, Hemamali Tennakoon, Jean Noel Ezingeard, The role of security notices and online consumer behaviour: An empirical study of social networking users, International Journal of Human Computer Studies;Aug 2015; 80:36-44.
6. Yuan Li.Theories in online information privacy research: A critical review and an integrated framework, Decision Support System. June 2012; 54(1):471-481.
7. Nader Yahya Alkeinay, Norita Md. Norwawi. User Oriented Privacy Model for Social Networks. International Conference on Innovation, Management and Technology Research, Malaysia; 22 – 23 September, 2013; 191-197.
8. Gail-Joon Ahn, Mohamed Shehab, Anna Squicciarini. Security and Privacy in Social Networks. IEEE Internet Computing; 2011; 15(3): 10- 12.
9. Paul Lowry, Jinwei Cao, Andrea Everard. Privacy Concerns versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. Journal of Management Information Systems; 2011; 27(4):163-200.
10. Carl Timm, Richard Perez. Seven Deadliest Social Network Attacks. Syngress Publishing; 2010.