Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

Security and privacy of social network users: investigation of individual factors

Khadije Akar [1] | **Mohammad Reza Kiani** [2] | **Mahmood Sangari** [3]

1. Master of Knowledge and Information Science, Faculty of Education and Psychology, University of Birjand, Birjand, Iran. (Corresponding Author) **E- mail**: akar_khadije@birjand.ac.ir
2. Assistant Professor, Department of Knowledge and Information Science, Faculty of Education and Psychology, University of Birjand, Birjand, Iran. **E- mail** :kiani.mreza@birjand.ac.ir
3. Assistant professor, Department of Library and Information Science, Faculty of Psychology and Educational Sciences, University of Birjand, Birjand, Iran. **E-mail:** msangari@birjand.ac.ir.

Article Info

Article type:
Research Article

Article history:
Received 9 May 2024
Received in revised form 23 June 2024
Accepted 15 August 2024
Published online 15 September 2024

Keywords:
individual factors,
Behavior,
security,
Social Networks.

ABSTRACT

The huge volume of data and information circulating in social networks, along with their popularity and widespread use, exposes these networks to numerous security risks. This descriptive survey used a Researcher-made questionnaire on a sample of students of University of Birjand (375 participants). For questionnaire's validity, the experts' opinions was used, and Cronbach's alpha was used for questionnaire's reliability (0.876). The average of users' overall awareness of security and privacy in social networks was significantly less than the optimal level, while the average of users' overall importance of security and privacy in social networks was higher than the optimal level. Also, the mean of attack experience variables, successful privacy changes, visit frequency, technological ability and skills, and perceived ease were significantly lower than desired; But the variables of trust in the system, perceived benefit, perceived risk and perceived importance were significantly more than the desired level. The amount of behaviors related to individual factors among the respondents was lower than expected. Although the respondents attached great importance to topics related to security and privacy, their awareness of many of these topics was less than expected. Also, the subjects of this research did not perform the behaviors related to individual factors related to security and privacy in social networks as expected.

Cite this article: Akar, Khadije., Kiani, Mohammd Reza., & Sangari, Mahmood. (2024). Security and privacy of social network users: investigation of individual factors. *Human-Information Interaction*, 11(2), 123-143.

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

Extended Abstract

Introduction

Online social networks are new and innovative media that have made changes in the social, cultural, economic and political structures of societies. These networks have not only changed the rules and regulations governing communication and interaction between humans, but also our thinking and attitude towards ourselves, others and the world. With the rapid development of technology, online social networks have become very popular in the current decade.

With the development of virtual space and the use of social networks, privacy is at risk more than ever, and in the meantime, social networks have a privileged status in terms of obtaining, collecting and using personal information. There are several security and privacy issues related to shared user information, especially when a user uploads personal content such as photos, videos, and audio files.

Methods and Materoal

This descriptive survey used a Researcher-made questionnaire on a sample of students of University of Birjand (375 participants). For questionnaire's validity, the experts' opinions was used, and Cronbach's alpha was used for questionnaire's reliability (0.876).

Resultss and Discussion

The increasing daily use of online social networks around the world leads to more problems regarding the security and privacy behavior of users in this attractive environment. While users can enjoy many benefits by using the service, at the same time they have many concerns about the privacy of their information. Despite privacy concerns, users continue to use these platforms and continue to share or self-disclose more personal information. Now, in order to deal with these threats, it is necessary to know what factors affect the security and privacy in social networks. According to many researches that have been conducted in this field, there are many factors that influence, but the factors that the current research focused on (after examining the level of awareness and importance of users to the two categories of security and privacy), two factors are individual factors and social engineering. was Individual factors being the factors that caused users to fail to use private settings, and social engineering was actually the abuse of trust or the deception of human agents to access confidential information and then abuse this information.

The results showed that although the respondents attached great importance to topics related to security and privacy, they admitted that they were less aware of many of these topics than expected. The results of the next questions showed that the behaviors related to individual factors were less than expected among the respondents, while the behaviors related to social engineering were within the expected range and even beyond. Examining the demographic variables showed that women received a higher score than men in all the investigated variables. Also, the scores of undergraduate students from two levels higher than theirs were higher in all variables.

Conclusion

In today's interconnected world, many relationships and interactions with others are virtual and they have provided easy conditions for exchanging information, news, events with the ability to comment and share information with a wide audience and even create content. Therefore, social media has attracted more and more attention. This volume of information exchange has put the security and privacy of users in social networks at risk. To deal with these threats, users must know what factors affect security and privacy. Among the broad

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/
Human-Information INTERACTION

factors that have been mentioned in previous studies, the most important factors have been discussed in the current research, which can be called individual factors and social engineering. Now, considering the need to clarify the issue, in this research, the role of individual factors and social engineering in the behaviors related to the security and privacy of users in social networks has been discussed.

The results of the questions confirmed that students, as active members of the society, are not as aware of issues related to security and privacy as they should be, and the percentage of this awareness was less than expected, but contrary to their relatively low awareness, fortunately, security and privacy are very important. They were private in social networks. Although it was expected that students, as an informed and cultured segment of the academic community, would have acceptable knowledge in the field of security and privacy, but unfortunately, the result of the present study was the opposite, and this is an alarm for all university and government officials who think about education and to inform the students.

On the other hand, it is true that students attach great importance to their security and privacy in social networks, but certainly to realize this issue and actually its prerequisite, to be familiar with the rules of the privacy policy and how to make security and privacy settings. It is that until this important thing is not done correctly, the issue of giving importance to security and privacy cannot be given proper attention, even though this issue is important for students.

Keywords: Keywords: individual factors; Behavior; security; Privacy; Social Networks

نشریه تعامل انسان و اطلاعات
https://hii.khu.ac.ir/
شاپا الکترونیکی: ۲۴۲۳-۷۴۱۸
دانشگاه خوارزمی

امنیت و حریم خصوصی کاربران شبکه‌های اجتماعی: بررسی عوامل فردی

خدیجه آکار[1]✉، محمدرضا کیانی[2]، محمود سنگری[3]

۱. نویسنده مسئول: کارشناس ارشد، علم اطلاعات و دانش شناسی، دانشکده علوم تربیتی و روانشناسی، دانشگاه بیرجند، بیرجند، ایران. akar_khadije@birjand.ac.ir

۲. استادیار، گروه علم اطلاعات و دانش‌شناسی، دانشکده علوم‌تربیتی و روانشناسی، دانشگاه بیرجند، بیرجند، ایران. رایانامه: kiani.mreza@birjand.ac.ir

۳. استادیار، گروه علم اطلاعات و دانش‌شناسی، دانشکده علوم‌تربیتی و روانشناسی، دانشگاه بیرجند، بیرجند، ایران. رایانامه: msangari@birjand.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۰۲/۲۰
تاریخ بازنگری: ۱۴۰۳/۰۴/۰۳
تاریخ پذیرش: ۱۴۰۳/۰۵/۲۵
تاریخ انتشار: ۱۴۰۳/۰۶/۱۵

کلیدواژه‌ها:
عوامل فردی،
رفتار،
امنیت،
حریم خصوصی،
شبکه‌های اجتماعی.

چکیده

زمینه و هدف: حجم عظیم‌داده‌ها و اطلاعات در حال گردش در شبکه‌های اجتماعی در کنار محبوبیت و گستردگی استفاده از آن‌ها، این شبکه‌ها را در معرض خطرات امنیتی متعددی قرار می‌دهد. بنابراین امروزه امنیت و حریم خصوصی کاربران به یکی از مهم‌ترین مسائل در شبکه‌های اجتماعی تبدیل شده است. عوامل زیادی بر روی امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی اثرگذارند که این پژوهش از آن میان، به بررسی نقش عوامل فردی در رفتارهای مرتبط با امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی پرداخته است.

روش‌پژوهش: روش این پژوهش کاربردی، توصیفی (از نوع پیمایشی) بود. گردآوری داده‌ها با استفاده از پرسش‌نامه محقق ساخته و در نمونه‌ای به حجم ۳۷۵ نفر از جامعه دانشجویان کارشناسی و کارشناسی ارشد و دکتری دانشگاه بیرجند و به روش نمونه‌گیری تصادفی طبقاتی نسبتی انجام شد. روایی پرسش‌نامه با تأیید متخصصان موضوعی و اساتید حاصل و برای آزمون پایایی از آزمون آلفای کرونباخ (۰/۸۷۶) استفاده شد.

یافته‌ها: میانگین میزان آگاهی کلی کاربران از امنیت و حریم خصوصی در شبکه‌های اجتماعی به طور معناداری کمتر از حد مطلوب بود در حالی‌که میانگین میزان اهمیت‌دادن کلی کاربران به امنیت و حریم خصوصی در شبکه‌های اجتماعی بیشتر از حد مطلوب بود. میزان انجام رفتارهای مرتبط با عوامل فردی در نزد پاسخگویان کمتر از حد انتظار بود. همچنین میانگین متغیرهای تجربه حمله، تغییرات موفقیت‌آمیز حریم خصوصی، دفعات بازدید، توانایی و مهارت‌های فناوری و سهولت درک شده به طور معناداری کمتر از حد مطلوب به دست آمد؛ اما متغیرهای اعتماد به سامانه، سود درک شده، خطر درک شده و اهمیت درک شده به طور معناداری بیشتر از حد مطلوب بود. علاوه بر این بررسی متغیرهای جمعیت‌شناختی نشان داد که در همه متغیرهای مورد بررسی بانوان نمره بالاتری از آقایان دریافت کردند. همچنین نمره دانشجویان کارشناسی از دو مقطع بالاتر از خودشان، در همه متغیرها بیشتر بود.

نتیجه‌گیری: اگرچه پاسخگویان برای مباحث مرتبط با امنیت و حریم خصوصی اهمیت زیادی قائل بودند، اما آگاهی آن‌ها به بسیاری از این مباحث کمتر از حد انتظار بود. همچنین آزمودنی‌های این پژوهش در حدی که انتظار می‌رفت، رفتارهای مربوط به عوامل فردی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی را انجام نمی‌دادند.

استناد: آکار، خدیجه؛ کیانی، محمدرضا؛سنگری، محمود (۱۴۰۳). امنیت و حریم خصوصی کاربران شبکه‌های اجتماعی: بررسی عوامل فردی. *تعامل انسان و اطلاعات*، ۱۱(۲)، ۱۲۳-۱۴۳.

مقدمه

رواج فناوری اطلاعات و ارتباطات، اشـــکال جدیدی از تعامل، از جمله خدمات شـــبکه اجتماعی آنلاین را امکان‌پذیر کرد. شـبکه‌های اجتماعی آنلاین به بخشـی جدایی‌ناپذیر از زندگی روزمره تبدیل شـده‌اند که افراد را با دوسـتان و خانواده ارتباط می‌دهد و اطلاعات را به اشـــتراک می‌گذارد (میتال[1]، ۲۰۲۳). شـــبکه‌های اجتماعی در واقع پلتفرم‌های آنلاینی هســـتند که کاربران از آن‌ها برای ایجاد شـــبکه‌های اجتماعی یا ارتباطات با افراد دیگر با دیدگاه‌ها، علایق، فعالیت‌ها و مخاطبین مشـــابه اســـتفاده می‌کنند (نواز و همکاران[2] ، ۲۰۲۳). بنابراین حجم وســـیعی از داده‌ها و اطلاعات در این فضـــا توســـط کاربران به اشـتراک گذاشـته می‌شـود. طبق گزارش سـایت اسـتتیسـتا در سـال ۲۰۲۳، بیش از ۴/۸۹ میلیارد نفر در سـراسـر جهان از رسانه‌های اجتماعی استفاده می‌کردند که پیش‌بینی می‌شود این رقم در سال ۲۰۲۷ به تقریباً شش میلیارد افزایش یابد. در ژانویه ۲۰۲۳ تعداد کاربران فعال فیس‌بوک ۲۹۵۸ میلیون، یوتیوپ ۲۵۱۴ میلیون، واتســـاپ ۲۰۰۰ میلیون، اینســـتاگرام ۲۰۰۰ میلیون، تلگرام ۷۰۰ میلیون و توئیتر ۵۵۶ میلیون نفر است. سوءاستفاده از این اطلاعات می‌تواند در دنیای مجازی و حقیقی آســـیب‌هایی به همراه داشـــته باشـــد (قضـــاوتی و نوروزی،۱۳۹۶). تا به امروز، شـــبکه‌های اجتماعی آنلاین مانند فیس‌بوک، توییتر و سـایر شـبکه‌های اجتماعی، به طور قابل‌توجهی مورد حمله قرار گرفته و پیامدهای قابل‌توجهی داشـته است. گاهی اوقات ممکن است مهاجم به داده‌های یک کاربر خاص آسیب نرساند، اما همچنان می‌تواند به طور خطرناکی بر عملیات کلی شـبکه‌های اجتماعی تأثیر بگذارد. در پی رسـوایی نقض اطلاعات فیس‌بوک، کاربران متوجه شـدند که داده‌های شـخصـی آن‌ها چقدر آسـیب‌پذیر اسـت و چقدر کورکورانه به شـبکه‌های اجتماعی آنلاین اعتماد می‌کنند (وانگ[3]،۲۰۲۰). بر اســـاس چنین رویدادهایی می‌توان گفت که شـــبکه‌های اجتماعی بهترین ابزار برای مهاجمان مخرب برای ارتکاب جرایم سـایبری هسـتند و امنیت و حریم خصـوصـی یکی از مهم‌ترین مسـائل در شـبکه‌های اجتماعی آنلاین اسـت که موردتوجه نهادهای امنیتی قرار گرفته است (نواز و همکاران، ۲۰۲۳).

امنیت با الهام از ریشه لاتین کلمه«*se + cura*» ، به معنای عاری از ترس یا اضطراب است و از چهاراصل اساسی تشکیل شده است:

۱. امنیت به عنوان یک آزادی. امنیت ممکن اســـت به عنوان آزادی مشـــترک از ترس و نیاز، و آزادی برای زندگی باعزت درک شود. این به‌جای عدم وجود خطر، به‌سلامت اجتماعی و زیست‌محیطی دلالت دارد.

۲. امنیت به‌عنوان یک حق مشـترک. تعهد به اشـتراک امری ضـروری اسـت. امنیت نباید و معمولاً نمی‌تواند برای گروهی از مردم با هزینه دیگران به دست آید. براین‌اساس، امنیت به‌جای تسلط، بر همبستگی استوار است (در کنار دیگران ایستادن، نه بالای سر آن‌ها).

۳. امنیت به‌عنوان یک عمل بیمار. امنیت باتوجه‌به اینکه جامعه چقدر فراگیر و عادلانه اســـت و چقدر از نظر اجتماعی و زیست‌محیطی مسئولیت‌پذیر هستیم، رشد می‌کند یا کم می‌شود.

۴. امنیت به‌عنوان یک مسئولیت مشترک. امنیت یک مسئولیت مشترک است. چالش‌های آن متعلق به همه ماست (گی[4]، ۲۰۱۶).

علاوه بر این امنیت از اینکه اطلاعات کاربر در دسـترس افراد غیرمجاز و سـوءاسـتفاده آنان قرار بگیرد محافظت می‌کند. در شـبکه‌های اجتماعی، اطلاعاتی از کاربران وجود دارد که بخشـی از این اطلاعات به حریم خصـوصـی آن‌ها مربوط می‌شـود و خطر فاش‌شدن یا سرقت این اطلاعات، تهدیدی برای حریم خصوصی آن‌ها است (نواز و همکاران،۲۰۲۳). حریم خصـوصـی به اطلاعات حسـاس شـخصـی و یا اجتماعی افراد اشـاره دارد و میزان کنترل دسـترسـی دیگران به این نوع اطلاعات را مورد

[1] Mittal
[2] Nawaz and etal
[3] Wang
[4] Gee

توجه قرار می‌دهد. برای مقابله با این تهدیدات، در مقابل، ارائه‌دهندگان شبکه‌های اجتماعی تنظیماتی برای حریم خصوصی ایجاد می‌کنند (کانامپیو[1]، ۲۰۱۸) و طبق مطالعات انجام شده (از جمله هو و همکاران[2]، ۲۰۱۸؛ کانامپیو، ۲۰۱۸؛ استرت[3]، ۲۰۱۹) برای شبکه‌های اجتماعی، داشتن تنظیمات کنترل دسترسی دقیق ضروری است.

عوامل زیادی (از جمله عوامل انسانی، فردی، معنوی، اجتماعی، مادی، رفتارهای مهندسی اجتماعی و ...) بر روی امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی اثرگذارند که تمرکز این مطالعه بر روی عوامل فردی است. عوامل فردی (شامل: تجربه حمله، دفعات بازدید، تغییرات موفقیت‌آمیز حریم خصوصی، اعتماد به سامانه، اهمیت درک شده، سود درک شده، خطر درک شده، توانایی و مهارت‌های فناوری، درک از امنیت و سهولت درک شده) عواملی بودند که به کوتاهی کاربران در استفاده از تنظیمات خصوصی منجر می‌شود (کانامپیو، ۲۰۱۸). تحقیقات زیادی نشان داده که کاربران معمولاً در تنظیمات حریم خصوصی مناسب کوتاهی می‌کنند (از جمله العبدالطیف و آلتوری[4]، ۲۰۱۸؛ کانامپیو، ۲۰۱۸؛ جین و همکاران،۲۰۲۱؛ احسانی‌فر، رضوانیان، ۱۳۹۶؛ حسین‌پور و مصرخانی،۱۳۹۷؛ جلالی و همکاران، ۱۳۹۶). نتیجه این کوتاهی، نقض حریم خصوصی آنلاین توسط هکرها و افراد سودجوست که باید از افراد در برابر این حملات محافظت شود (مورد تأکید در پژوهش‌های گوپتا و همکاران، ۲۰۱۸؛ کرامبهلز و همکاران[5]، ۲۰۱۵؛ پورنقدی، ۱۳۹۷). در شبکه‌های اجتماعی، نقض حریم خصوصی عمدتاً ناشی از رفتار کاربران آنلاین است (البلادی و ویر[6]،۲۰۲۰؛ کلنامپیو،۲۰۱۸؛ آلبلادی و ویر،۲۰۱۸). یکی از این رفتارها سهل‌انگاری و کوتاهی در تنظیمات حریم خصوصی مناسب برای پروفایل‌های کاربر است که بررسی عواملی مانند تجربه حمله، دفعات بازدید، تغییرات موفقیت‌آمیز حریم خصوصی باعث این کوتاهی می‌شود. برخی از کاربران محبوبیت و قابلیت استفاده را به جای امنیت و حریم خصوصی ترجیح می‌دهند، ازاین‌رو این موارد نادیده گرفته می‌شوند و بعضی به تنظیمات حریم خصوصی و سیاست حفظ حریم خصوصی و شرایط خدمات در شبکه‌های اجتماعی بی‌توجهی نشان می‌دهند (کانامپیو، ۲۰۱۸؛ علی و همکاران[7]، ۲۰۱۸) و عدم آگاهی کاربران در این زمینه، این پتانسیل را دارد که منجر به حملات سایبری مختلف از طریق رسانه‌های اجتماعی شود. همچنین الحسیب (۲۰۰۹) یک دسته از تهدیدهای بالقوه‌ای که کاربران شبکه‌های اجتماعی ممکن است با آن مواجه شوند تهدیدات مربوط به حریم خصوصی (از قبیل پرونده دیجیتال اطلاعات شخصی، تشخیص چهره، بازیابی تصویر مبتنی بر محتوا، برچسب‌گذاری تصویر و پروفایل متقابل و دشواری حذف کامل حساب) می‌داند. در دسته‌بندی دیگری نواز و همکارانش (۲۰۲۳) یکی از تهدیدات شبکه‌های اجتماعی را تهدیدات چندرسانه‌ای‌ها می‌دانند که کاربران با به اشتراک گذاشتن و فیلم و تصاویر خود در این فضاها باعث تهدیداتی مثل افشای غیرمجاز داده، شبیه‌سازی هویت، مکان‌یابی کاربر، سرقت هویت و... می‌شوند.

از این رو نقش عوامل فردی در رابطه با امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی بسیار پررنگ جلوه می‌کند. وجود پژوهشی که بیانگر نقش این عوامل باشد، به کاربران کمک شایانی می‌کند تا بهتر بتوانند خود را در برابر خطرات امنیتی و حریم خصوصی در شبکه‌های اجتماعی ایمن سازند و در صورت مواجهه با اینگونه خطرات از خود محافظت کنند. لذا پژوهش حاضر به این مسئله می‌پردازد و به دنبال آن است تا دریابد که آیا کاربران از این عوامل مطلع هستند؟ و به آن‌ها اهمیت داده‌اند؟ و اگر بله میزان این اطلاع و اهمیت چقدر بوده است؟ در کنار این موارد دریابد که آیا کاربران این عوامل را در رفتارهای خود انجام داده‌اند؟ و در نهایت نقش متغیرهای جمعیت‌شناختی در این رابطه چقدر بوده است؟

[1] Kanampiu
[2] Hu and etal
[3] Steiert
[4] Abdullah and Alturise
[5] Krombholz and etal
[6] Albladi & weir
[7] Ali and at al

پیشینه پژوهش

یافته‌های پژوهش‌هایی که به مسئله امنیت و حریم خصوصی در شبکه‌های اجتماعی پرداخته‌اند، نشان داد با توسعه فضای مجازی و استفاده از شبکه‌های اجتماعی، مسائل امنیتی و حریم خصوصی متعددی در رابطه با اطلاعات به اشتراک گذاشته شده کاربر وجود دارد و تهدیدات بسیاری متوجه آن‌هاست و کاربران نگران این مسئله هستند. برخی از پژوهش‌های اخیر در این زمینه عبارتند از: میتال،۲۰۲۳ (درک کاربران از حریم خصوصی و امنیت در شبکه‌های اجتماعی آنلاین)؛ حسینی سنو و مظاهری، ۱۳۹۷ (حریم خصوصی، امنیت و اعتماد ادراک شده بر رفتار به‌اشتراک‌گذاری اطلاعات در شبکه‌های اجتماعی موبایل)؛ حسین‌پور و مصرخانی، ۱۳۹۷ (نقش شبکه‌های اجتماعی بر امنیت عمومی کاربران)؛ البلادی و ویر،۲۰۲۰ (آسیب پذیری افراد در برابر مهندسی اجتماعی در شبکه‌های اجتماعی)؛ جلالی و همکاران، ۱۳۹۶ (مدیریت حریم شخصی کاربران) ؛ جین و همکاران[1]،۲۰۲۱) امنیت و حریم خصوصی شبکه‌های اجتماعی آنلاین)؛ نواز و همکاران،۲۰۲۳(تهدیدات امنیتی و راه‌حل‌های شبکه‌های اجتماعی آنلاین)؛ گی، ۲۰۱۶(امنیت)؛ کلنامپیو، ۲۰۱۸(امنیت و حریم خصوصی در شبکه‌های اجتماعی آنلاین و دیدگاه عوامل انسانی)؛ هو و همکاران، ۲۰۱۸ (اشتراک‌گذاری تصایر دیجیتال در شبکه‌های اجتماعی)؛ استرت، ۲۰۱۹ (حفظ حریم خصوصی در شبکه‌های اجتماعی موبایل)؛ ذوالفهمی و همکاران[2]،۲۰۲۲) حفاظت از حریم خصوصی در رسانه‌های اجتماعی)؛ یی و همکاران[3]،۲۰۲۳) اثرات استفاده از رسانه‌های اجتماعی بر تنهایی و رفاه)؛ شایک و همکاران[4]، ۲۰۱۸) امنیت و حریم خصوصی در شبکه‌های اجتماعی آنلاین)؛ ژانگ و همکاران[5]، ۲۰۲۲ (امنیت شبکه‌های اجتماعی آنلاین). علیرغم این نگرانی برخی پژوهش‌های تکمیلی مانند بهاتناگار و پرای[6] (۲۰۲۰) با عنوان نگرش، آگاهی و درک دانشجویان از حریم خصوصی و امنیت سایبری نشان داد که اگرچه کاربران از خطرات موجود در رسانه‌های اجتماعی آگاه هستند اما درک و استفاده از تنظیمات امنیتی رسانه‌های اجتماعی سخت است و معمولا نادیده گرفته می‌شود.

علاوه بر این پژوهش‌های انجام شده در مورد عوامل فردی به شرح زیر است:

اولین عامل فردی تجربه حمله بود که می‌توان به پنسا و بلسی[7] (۲۰۱۷) (درک کاربران از حریم خصوصی و امنیت در شبکه‌های اجتماعی آنلاین)، نیفاکوس و همکاران[8] (۲۰۲۱) (تأثیر عوامل انسانی بر امنیت سایبری)، البلادی و ویر[9] (۲۰۱۸) (تأثیرگذاری ویژگی‌های کاربر بر حملات مهندسی اجتماعی در شبکه‌های اجتماعی) و اسکرودر[10] (۲۰۱۹) (مهندسی اجتماعی و آسیب‌پذیری‌های انسانی) اشاره کرد که به طور کلی به این نتیجه رسیدند که گروه‌هایی که خطر را تجربه کرده بودند و تجربه شخصی حمله داشتند در شناسایی تهدید موفق تر بودند و میزان آسیب‌پذیری کمتری را در برابر تهدیدات تجربه کردند.

عامل فردی بعدی تغییرات موفقیت‌آمیز حریم خصوصی بود. سانی[11] (۲۰۲۳) (بررسی رفتار حریم خصوصی روزنامه‌نگاران در تاریخ‌های وضعیت واتساپ در ایالت کانو) و (ریچل و همکاران[12] (۲۰۲۰)(درک برداشت کاربران از حریم خصوصی و رفتارهای فعلی در فیس‌بوک و واتساپ) به این نتیجه رسیدند که کاربران تنظیمات حریم خصوصی خود را ویرایش می‌کنند

[1] Jain and et al
[2] Zulfahmi and etal
[3] Yi and et al
[4] Van Schaik and at al
[5] Zhang and et al
[6] Bhatnagar & Pry
[7] Pensa & Blasi
[8] Nifakos and et al
[9] Albladi & Weir
[10] Schroeder
[11] Sani
[12] Reichel and et al

تا کنترل کنند که چه کسانی پیام‌ها یا پست‌های آن‌ها را می‌بینند. طبق پژوهش اوبار و هیرش[1] (۲۰۱۸) با عنوان «نادیده‌گرفتن سیاست‌های حفظ حریم خصوصی و خط‌مشی‌های خدمات شبکه‌های اجتماعی» شرکت‌کنندگان به سیاست‌های حریم خصوصی به‌عنوان مزاحم نگاه می‌کنند و اما در مقابل ایساک و هاناک[2] (۲۰۱۸) با عنوان «بررسی حریم خصوصی داده‌های کاربر فیس‌بوک و کمبریج آنالیتیکا و حفاظت از حریم خصوصی» به این نتیجه رسیدند که تدوین قوانین جامع سیاست حفظ حریم خصوصی ضروری است.

در نهایت از پژوهش‌های انجام شده در مورد سایر عوامل فردی می‌توان به این موارد اشاره کرد: میتال، ۲۰۲۳ (اعتماد به سامانه، توانایی و مهارت‌های فناوری، سهولت درک شده، اهمیت درک شده)؛ فریک و همکاران[3]، ۲۰۲۲ (توانایی و مهارت های فناوری)؛ آلجدانی و همکاران[4]، ۲۰۲۳ (توانایی و مهارتهای فناوری)؛ حسینی و و مظاهری، ۱۳۹۷ (اعتماد به سامانه و اهمیت درک شده)؛ یورو و همکارانش[5]، ۲۰۲۳ (اعتماد به سامانه)؛ مارتین ناوالون و همکارانش[6]، ۲۰۲۳ (اهمیت درک شده، اعتماد به سامانه، سهولت درک شده)؛ یسا و همکاران[7]، ۲۰۲۳ (سود درک شده)؛ تانگو و نینگ[8]، ۲۰۲۳ (سود درک شده)؛ جین و همکاران، ۲۰۲۱ (سود درک شده)؛ اسچیف و فلووردی[9]، ۲۰۲۱ (دفعات بازدید)؛ کانامپیو، ۲۰۱۸ (دفعات بازدید، توانایی و مهارت)؛ ذوالفهمی و همکاران، ۲۰۲۳ (دفعات بازدید)؛ چویی[10]، ۲۰۲۳ (خطر درک شده)؛ ریچل و همکاران، ۲۰۲۰ (خطر درک شده)؛ البلادی و ویر، ۲۰۲۰ (اهمیت درک شده، اعتماد به سامانه)؛ کوسیانتی و همکاران[11]، ۲۰۲۲ (سود درک شده و سهولت درک شده)؛ سعید[12]، ۲۰۲۳ (سود درک شده)؛ وی و همکاران[13]، ۲۰۲۲ (اهمیت درک شده، اعتماد به سامانه، توانایی و مهارت های فناوری). براین اساس، پژوهش حاضر به دنبال پاسخ به این پرسش‌ها هست:

میزان آگاهی کاربران از مباحث مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی چقدر است؟

میزان اهمیت دادن کاربران به مباحث مرتبط با امنیت و حریم خصوصی در شبکه های اجتماعی چقدر است؟

میزان انجام رفتارهای مربوط به عوامل فردی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی توسط کاربران چقدر است؟

متغیرهای جمعیت‌شناختی (جنسیت، تحصیلات) به چه میزان بر رفتارهای مرتبط با امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی اثرگذارند؟

روش پژوهش

این پژوهش کاربردی و توصیفی در نمونه‌ای به حجم ۳۷۵ نفر از جامعه دانشجویان دانشگاه بیرجند به روش نمونه‌گیری تصادفی طبقاتی نسبتی انجام شد. جامعه مورد مطالعه دانشجویان دانشگاه بیرجند (۱۰۵۳۴ نفر) بودند. ۱۸۳ نفر از شرکت‌کنندگان زن و ۱۹۲ نفر مرد بودند. ۲۳۷ دانشجو در مقطع کارشناسی، ۱۱۰ دانشجو در مقطع کارشناسی ارشد و ۲۸ دانشجو در مقطع دکتری مشغول به تحصیل بودند. لازم به توضیح است طبقات نمونه براساس مقطع تحصیلی محاسبه شد. داده‌های پژوهش با استفاده پرسش‌نامه محقق ساخته گردآوری شد. پرسش‌نامه شامل ۲۱ گویه است و از طیف لیکرت در آن استفاده شد (از ۱ به معنای کاملا مخالفم تا ۵ به معنای کاملا موافقم نمره‌گذاری شد). پرسش‌نامه از پنج بخش تشکیل

[1] Obar & Oeldorf-Hirsch
[2] Isaak & Hanna
[3] Frik and et al
[4] Aljedaani and et al
[5] Yoro and et al
[6] Martínez-Navalón and et al
[7] Yisa and et al
[8] Tang & Ning
[9] Van der Schyff & Flowerday
[10] Choi
[11] Kusyanti and et al
[12] Saeed
[13] Wei and et al

شـده‌اسـت که مبنای آن برآوردن هدف‌ها و پاسـخ به سـؤالات پژوهش اسـت. بخش اول و دوم در مورد آگاهی از امنیت و آگاهی از حریم خصـوصـی، بخش سـوم و چهارم در مورد اهمیت امنیت و اهمیت حریم خصـوصـی و بخش پنجم در مورد عوامل فردی بود. تجزیه و تحلیل داده‌های آماری این پژوهش با استفاده از روش‌های آمار توصیفی (میانگین، انحراف معیار، جداول و نمودارها) و آمار اسـتنباطی (شـامل آزمون‌های تی تک نمونه، تی مسـتقل، من ویتنی، دوجمله‌ای، تحلیل واریانس یک طرفه و کروسکال والیس) با استفاده از نرم‌افزار اس پی اس اس انجام شد. ضمناً نرمال بودن توزیع داده‌ها با استفاده از آزمون کولموگروف- اسمیرنوف مورد تأیید قرار گرفت.

یافته‌های پژوهش

سؤال اول: میزان آگاهی کاربران از مباحث مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی چقدر است؟

یافته‌ها نشان داد که آگاهی دانشجویان نسبت به مسائل امنیتی و حریم خصوصی خود در شبکه‌های اجتماعی از حد انتظار پژوهشگران که به عنوان حد مطلوب تعریف شده بود، کمتر بود.

جدول ۱. نتایج آزمون مقایسه میانگین میزان آگاهی کاربران از امنیت و حریم خصوصی در شبکه‌های اجتماعی با حد مطلوب

متغیر	میانگین	انحراف معیار	حد مطلوب	تفاوت میانگین	T	Df	سطح معناداری
آگاهی از امنیت	۹۴/۸	۰۷۹/۳	۱۲	-۰۶/۳	۲۷۴/۱۹	۳۷۴	۰/۰۰۰۱
آگاهی از حریم خصوصی	۶۳/۹	۱۴۳/۳	۱۲	-۲/۳۶۶	-۵۶۰/۱۴	۳۷۳	۰/۰۰۰۱
آگاهی از امنیت و حریم خصوصی	۵۶/۱۸	۸۲/۵	۲۴	-۴۴/۵	-۱۸/۰۷	۳۷۳	۰/۰۰۰۱

طبق یافته‌های بونیش و همکاران[1] (۲۰۲۱) آگاهی عمومی نسبتاً پایینی از امنیت و حریم خصوصی در میان پزشکان وجود دارد. آلجدانی و همکاران (۲۰۲۳) نیز بیان کردند اکثر کاربران نهایی از ویژگی‌های امنیتی موجود (مانند مجوزهای محدود برنامه) اطلاع ندارند. همچنین اکوکپوجی[2] (۲۰۲۳) در پژوهش خود به این نتیجه رسید که ۷۰/۶ درصد از دانشجویان مورد بررسی به دلیل ناآگاهی مستعد حملات فیشینگ در محیط دانشگاهی هستند.

پژوهش‌های دیگری در خارج و داخل از کشـــور از قبیل کورین و همکاران[3] (۲۰۲۳)؛ نیونی و ولمپینی[4] (۲۰۱۸)؛ علنی[5] (۲۰۱۷)؛ الحســـیب[6] (۲۰۰۹)؛ گربر و همکاران[7] (۲۰۱۸)؛ فریک و همکاران[8] (۲۰۲۲)؛ رجب و همکاران[9] (۲۰۲۳) و آرین و همکاران[10] (۲۰۲۲) نتایجی همسو با نتایج پژوهش حاضر به دست آورده‌اند. تنها پژوهش ناهمسو مطالعه جلالی و همکاران (۱۳۹۶) بود. آن‌ها به این نتیجه رسـیدند که نزدیک به ۶۷ درصـد افراد از گزینه‌های امنیتی مربوط به حریم شـخصـی آگاه بودند.

سؤال دوم: میزان اهمیت دادن کاربران به مباحث مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی چقدر است؟

یافته‌ها پژوهش حاضـر نشـان داد که کاربران به مباحث مرتبط با امنیت و حریم خصـوصـی در شـبکه‌های اجتماعی اهمیت می‌دهند و در اکثر موارد این میزان بیشتر از حد انتظار بود.

[1] Boenisch and et al
[2] Okokpujie
[3] Korir and at al
[4] Nyoni & Velempini
[5] Alani
[6] Al Hasib
[7] Gerber and etal
[8] Frik and etal
[9] Ragab and etal
[10] Arain and etal

جدول ۲. نتایج آزمون مقایسه میانگین اهمیت‌دادن کاربران به امنیت وحریم خصوصی در شبکه‌های اجتماعی با حد مطلوب

متغیر	میانگین	انحراف معیار	حد مطلوب	تفاوت میانگین	T	Df	سطح معناداری
اهمیت دادن به امنیت	۱۳/۳۳	۲/۱۷۶	۱۲	۱/۳۳	باتوجه‌به نرمال نبودن از آزمون دوجمله‌ای استفاده شد		
اهمیت دادن به حریم خصوصی	۱۲/۱۶	۲/۵۲۱	۱۲	۰/۱۶۴	۱/۲۵۳	۳۷۲	۰/۲۱۱
اهمیت دادن به امنیت و حریم خصوصی	۲۵/۵۰	۴/۱۸۵	۲۴	۱/۴۹۳	۶/۸۹۰	۳۷۲	۰/۰۰۰۱

باتوجه‌به نرمال نبودن توزیع متغیر اهمیت - امنیت از آزمون معادل ناپارامتری دوجمله‌ای به‌جای آزمون تی تک نمونه استفاده شد.

جدول ۳. نتایج آزمون مقایسه میانگین اهمیت‌دادن کاربران به امنیت در شبکه‌های اجتماعی با حد مطلوب

متغیر	گروه‌بندی	تعداد	سطح معناداری
اهمیت دادن به امنیت	کوچکتر و مساوی ۱۲	۹۷	۰/۰۰۱
	بزرگتر از ۱۲	۲۷۸	

پژوهش‌های زیادی (از قبیل کوریر و همکاران (۲۰۲۳)؛ تانگو و نینگ (۲۰۲۳)؛ اکبر و همکاران[1] (۲۰۲۲)؛ کوآن‌هاسه و هو[2] (۲۰۲۰)؛ حسن و همکاران[3] (۲۰۲۰)؛ ریچل و همکاران (۲۰۲۰)؛ هو و همکاران (۲۰۱۸)؛ کلنامپیو (۲۰۱۸)) به نتایجی مشابه با نتایج این پژوهش دست‌یافته‌اند که به برخی از آن‌ها اشاره می‌شود. طبق پژوهش کوریر و همکاران (۲۰۲۳) دانشجویان نگران به اشتراک گذاشتن داده‌های خود با اشخاص ثالث بودند. همچنین تانگو و نینگ (۲۰۲۳) دریافتند که کاربران با درجه بالایی از نگرانی‌های مربوط به حریم خصوصی روبرو هستند. اکبر و همکاران (۲۰۲۲) معتقدند اکثریت شرکت‌کنندگان بسیار نگران مسائل حریم خصوصی و امنیتی بودند. همان‌طور که مشاهده شد تمامی نتایج حاکی از آن است که در فضای مجازی و شبکه‌های اجتماعی، کاربران نسبت به امنیت و حریم خصوصی خود نگران بوده و این مسئله برایشان بسیار حائز اهمیت است. اما نکته مهم آن است که آیا این نگرانی منجر به انجام رفتارهای مرتبط با امنیت و حریم خصوصی هم می‌شود یا خیر؟ سؤالی که پرسش سوم این پژوهش به دنبال پاسخ به آن است.

تنها پژوهش ناهمسو با پژوهش حاضر، متعلق به میر و کرامر[4] (۲۰۲۳) بود که دریافتند که نگرانی‌های مربوط به حریم خصوصی فردی آن‌قدر که گمان می رود، برای کاربران مهم نیستند.

سؤال سوم: میزان انجام رفتارهای مربوط به عوامل فردی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی توسط کاربران چقدر است؟

نتایج حاصل از آزمون تی تک نمونه نشان داد که میزان انجام رفتارهای مربوط به عوامل فردی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی به طور معناداری کمتر از حد مطلوب بود.

[1] Akbar and etal
[2] Quan-Haase & Ho
[3] Hassan and et al
[4] Meier & Krämer

جدول ۴. نتایج آزمون مقایسه میانگین میزان انجام رفتارهای مربوط به عوامل فردی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی

متغیر	میانگین	انحراف معیار	حد مطلوب	تفاوت میانگین	T	DF	سطح معناداری
عوامل فردی	۳۲/۷۶	۵/۳۲۲	۳۶	-۳/۲۳۹	-۱۱/۷۵۳	۳۷۲	۰/۰۰۰۱
تجربه حمله	۳/۳۰	۱/۲۷۰	۴	-۰/۶۹۹	-۱۰/۶۵۶	۳۷۴	۰/۰۰۰۱
تغییرات موفقیت‌آمیز حریم خصوصی	۳/۰۶	۱/۲۳۴	۴	-۰/۹۴۴	-۱۴/۸۱۰	۳۷۴	۰/۰۰۰۱
دفعات بازدید	۳	۱/۲۰۸	۴	-۱	-۱۶/۰۱۴	۳۷۳	۰/۰۰۰۱
اعتماد به سامانه	۴/۱۶	۰/۸۹۸	۴	-۰/۱۵۷	۳/۳۹۲	۳۷۴	۰/۰۰۱
توانایی و مهارت‌های فناوری	۱/۷۴	۰/۹۵۳	۴	-۲/۲۵۶	-۴۵/۸۵۸	۳۷۴	۰/۰۰۰۱
سود درک شده	۴/۲۳	۰/۹۵۵	۴	۰/۲۳۲	۴/۷۰۶	۳۷۴	۰/۰۰۰۱
سهولت درک شده	۳/۶۱	۱/۰۹۴	۴	-۰/۳۹۵	-۶/۹۸۶	۳۷۴	۰/۰۰۰۱
خطر درک شده	۴/۱۵	۱/۰۳۸	۴	۰/۱۵۰	۲/۷۹۱	۳۷۳	۰/۰۰۶
اهمیت درک شده	۴/۱۹	۰/۹۸۲	۴	۰/۱۸۷	۳/۶۸۰	۳۷۴	۰/۰۰۰۱

اولین عاملی فردی مورد بررسی، تجربه حمله بود. پژوهش هایی از قبیل البلادی و ویر (۲۰۲۰)؛ نیفاکوس و همکاران (۲۰۲۱)؛میتال (۲۰۲۳)؛ اسکرودر (۲۰۱۹)و چویی[1] (۲۰۲۳) نشان داده‌اند که عامل تجربه حمله یکی از مهم‌ترین عوامل فردی است که در امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی مؤثر است و انجام این رفتار باعث جلوگیری از به‌خطرافتادن کاربران در برابر مسائل امنیتی و حریم خصوصی می‌شود. اما برخلاف این مهم، طبق نتایج به‌دست‌آمده دانشجویان کمتر از حد انتظار این رفتار را انجام داده بودند.

عامل فردی بعدی که در پژوهش حاضر موردمطالعه قرار گرفت، تغییرات موفقیت آمیز حریم خصوصی بود. طبق نتایج پژوهش های اسچیف و فلووردی[2] (۲۰۲۱)؛ الحسیب (۲۰۰۹)؛ ایساک و هاناک (۲۰۱۸)؛ سورا و همکاران[3] (۲۰۲۳)؛ کانامپیو (۲۰۱۸) اکثرکاربران تنظیمات حریم خصوصی خود را ویرایش نمی‌کنند و در نقطه مقابل پژوهش های بهاتناگار و پرای (۲۰۲۰) و سانی(۲۰۲۰) اکثریت پاسخ‌دهندگان از ویژگی‌های امنیتی استفاده می‌کنند وتنظیمات حریم خصوصی را ویرایش می‌کنند.

عامل فردی بعدی، دفعات بازدید است. طبق پژوهش های صورت گرفته (اسچیف و فلووردی (۲۰۲۱)؛ کانامپیو (۲۰۱۸)؛ ذوالفهمی و همکاران (۲۰۲۳)) دانشجویان هر چه بیشتر به شبکه‌های اجتماعی خود سر بزنند باعث نمی‌شود که بیشتر به مسائل امنیتی و حریم خصوصی خود اهمیت دهند.

عامل دیگری که در پژوهش حاضر میزان انجام آن مورد بررسی قرار گرفت عامل توانایی و مهارت‌های فناوری بود. با توجه به نتایج پژوهش‌های (میتال (۲۰۲۳)؛ بونیش و باتیس (۲۰۲۱)؛ کوآن‌هاسه و هو (۲۰۲۰)؛ فریک و همکاران (۲۰۲۲)؛ آلجدانی و همکاران (۲۰۲۳)؛ ندلیکو و همکاران[4] (۲۰۲۱)؛ وی و همکاران[5] (۲۰۲۲)؛ کانامپیو (۲۰۱۸) شاید بتوان گفت در وهله اول برای محافظت از امنیت و حریم خصوصی در شبکه‌های اجتماعی حتما باید با روش های آن آشنا و از توانایی و مهارت های لازم برای به کارگیری آن‌ها برخوردار بود در غیر اینصورت نباید انتظار داشت که بتوان تا حدودی از خطرهای امنیتی و حریم خصوصی در امان باشیم. اما با وجود لزوم ضرورت داشتن توانایی و مهارتهای فناوری لازم در شبکه‌های اجتماعی، دانشجویان در پژوهش حاضر کمتر از حد مطلوب واجد این توانمندی بودند.

[1] Choi
[2] Schyff & Flowerday
[3] Saura and etal
[4] Nedeljko and etal
[5] Wei and etal

سهولت درک شده عامل فردی دیگری است که در این پژوهش به آن پرداخته شد. طبق پژوهش های میتال (۲۰۲۳)؛ مارتین ناوالون و همکاران (۲۰۲۳)؛ کوسیانتی و همکاران[1] (۲۰۲۲) وقتی استفاده از تلفن آسان باشد باعث می‌شود فرد تمایل بیشتری به ادامه استفاده از برنامه را داشته باشد.

اعتماد به سامانه عامل فردی بعدی است. پژوهش های البلادی و ویر (۲۰۲۰)؛ وی و همکاران (۲۰۲۲)؛ حسینی نو و مظاهری (۱۳۹۷)؛ میتال (۲۰۲۳)؛ مارتین ناوالون و همکاران (۲۰۲۳) به این نتیجه رسیدند که اعتماد کاربر به یک شبکه اجتماعی آنلاین یک مفهوم چند وجهی است که شامل اعتماد به نفس در توانایی این پلتفرم برای محافظت از اطلاعات شخصی و همچنین عواملی است که بر این اعتماد تأثیر می‌گذارد. عواملی مانند نقض داده‌ها، خط‌مشی داده‌ها و درک کاربران از امنیت آنلاین و حریم خصوصی می‌توانند نقش مهمی در ایجاد یا آسیب‌رساندن به اعتماد کاربر داشته باشند. شبکه‌های اجتماعی که در سیاست‌های خود شفاف هستند و پاسخگوی نگرانی‌های کاربر هستند می‌تواند باعث حفظ و کمک به اعتماد کاربر شوند. حال نتایج پژوهش حاضر و پژوهش‌های قبلی انجام شده موید موارد اشاره شده است و به طور مطلوب و مورد انتظار، اعتماد دانشجویان به سامانه منجر به کاهش تنظیمات حریم خصوصی و امنیتی نمی‌شد.

عامل فردی دیگری که به آن پرداخته شد عامل سود درک شده بود. با توجه به نتایج پژوهش‌های پنسا و بلسی (۲۰۱۷)؛ یسا و همکارانش (۲۰۲۳)؛ تانگو و نینگ (۲۰۲۳)؛ کوسیانتی و همکاران (۲۰۲۲)؛ اوبار و هیرش (۲۰۱۸) سود درک شده به طور مثبتی بر امنیت و حریم خصوصی تاثیر می‌گذارد. به عبارتی انجام تنظیمات امنیت و حریم خصوصی در شبکه‌های اجتماعی به زحمتش می‌ارزد.

خطر درک شده عامل فردی بعدی است که در پژوهش حاضر با اشاره به پژوهش‌های انجام شده، تحلیل می‌شود. چویی (۲۰۲۳) معتقد است تجربیات مربوط به ویژگی‌های حریم خصوصی باعث افزایش سواد حریم خصوصی می‌شود. همچنین ریچل و همکاران (۲۰۲۰) به این نتیجه رسیدند که نگرانی اصلی کاربران مربوط به حریم خصوصی این است که چه کسی می‌تواند پست‌ها و پیام‌های آن‌ها را ببیند و کاربران برای محافظت از حریم خصوصی به‌شدت به مسدودکردن و رمزهای عبور متکی هستند.

طبق نتایج پژوهش‌های ذکر شده انجام تنظیمات امنیت و حریم خصوصی در شبکه‌های اجتماعی از جمله موارد حیاتی است که نباید از آن غافل شده و نباید آن را جزء موارد ناچیز یا بی ارزش دانست بلکه با دقت در تنظیمات حفاظتی می‌توان از بسیاری از خطرات امنیتی و حریم خصوصی در امان ماند.

و آخرین عامل فردی، اهمیت درک شده است. پژوهش‌هایی از قبیل: سعید (۲۰۲۳)؛ ایساک و هاناک (۲۰۱۸)؛ مامونوو و بهبونان فیچ (۲۰۱۸)؛ جین و همکاران (۲۰۲۱) نشان داده‌اند که کاربران باید هنگام ارسال هرگونه رسانه یا اطلاعات در شبکه‌های اجتماعی هوشیار باشند، یک رمز عبور قوی باید اتخاذ شود و نباید با کسی به اشتراک گذاشته شود و با توجه به افشای اطلاعات بعضی کاربران، تدوین قوانین جامع سیاست حفظ حریم خصوصی ضروری است.

سؤال چهارم: متغیرهای جمعیت‌شناختی (جنسیت، تحصیلات)به چه میزان بر رفتارهای مرتبطبا امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی اثرگذارند؟

نتایج حاصل از آزمون تی مستقل نشان داد که میانگین همه متغیرها (آگاهی از امنیت، آگاهی از حریم خصوصی، اهمیت دادن به امنیت، اهمیت دادن به حریم خصوصی، عوامل فردی) در گروه زنان از گروه مردان، به طور معناداری بیشتر است. به عبارتی میزان آگاهی، اهمیت‌دادن و انجام رفتارهای مرتبط با امنیت و حریم خصوصی در بین زنان میانگین بالاتری را به دست آورده است.

[1] Kusyanti and at al

جدول ۵. نتایج آزمون مقایسه میزان رفتارهای مرتبط با امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی در بین زنان و مردان

متغیر	جنسیت	تعداد	میانگین	انحراف معیار	سطح معناداری آزمون لون	T	سطح معناداری آزمون T
آگاهی از امنیت	زن	۱۸۳	۹/۵۳	۲/۵۵۹	۰/۰۰۰۱	۳/۷۱۰	۰/۰۰۰۱
	مرد	۱۹۲	۸/۳۷	۳/۴۱۴			
آگاهی از حریم خصوصی	زن	۱۸۲	۱۰/۶۴	۲/۵۹۶	۰/۰۰۰۱	۶/۳۱۸	۰/۰۰۰۱
	مرد	۱۹۲	۸/۶۸	۳/۳۲۲			
آگاهی از امنیت و حریم خصوصی	زن	۱۸۲	۲۰/۱۵۹	۴/۷۳۲	۰/۰۰۰۱	۵/۳۵۰	۰/۰۰۰۱
	مرد	۱۹۲	۱۷/۰۵۲	۶/۳۳۶			
اهمیت دادن به امنیت	زن	۱۸۳	۱۳/۸۳	۱/۸۸۲	۰/۰۰۲	باتوجه‌به نرمال نبودن متغیر از آزمون من ویتنی استفاده شد.	
	مرد	۱۹۲	۱۲/۸۵	۲/۳۳۱			
اهمیت دادن به حریم خصوصی	زن	۱۸۱	۱۲/۸۱	۲/۲۱۶	۰/۰۱۶	۴/۹۷۵	۰/۰۰۰۱
	مرد	۱۹۲	۱۱/۵۵	۲/۶۴۲			
اهمیت دادن به امنیت و حریم خصوصی	زن	۱۸۱	۲۶/۶۴۶	۳/۷۳۲	۰/۰۱۸	۵/۳۵۵	۰/۰۰۰۱
	مرد	۱۹۲	۲۴/۴۰	۴/۳۰۶			
عوامل فردی	زن	۱۸۲	۳۴/۲۱	۴/۸۷۱	۰/۰۶۶	۵/۳۳۳	۰/۰۰۰۱
	مرد	۱۹۱	۳۱/۳۸	۵/۳۷۶			

باتوجه به نرمال نبودن توزیع متغیر اهمیت دادن به امنیت از آزمون معادل ناپارامتری من ویتنی به‌جای تی مستقل استفاده شد. ازآنجایی‌که سطح معناداری متغیر اهمیت - امنیت کوچکتر از ۰/۰۵ است میانگین متغیر به طور معناداری در بین زنان و مردان متفاوت است.

جدول ۶. نتایج جدول آزمون من ویتنی برای متغیر اهمیت - امنیت

متغیر	گروه‌بندی	تعداد	سطح معناداری
اهمیت دادن به امنیت	زن	۱۸۳	۰.۰۰۰۱
	مرد	۱۹۲	

برای بررسی تفاوت میانگین بین گروه‌های آزمودنی‌ها که بر اساس سطح تحصیلات دسته‌بندی‌شده بودند از آزمون تحلیل واریانس یک‌طرفه استفاده شد. نتایج نشان داد میانگین هیچ یک از متغیرها در سه گروه تحصیلی (کارشناسی، کارشناسی ارشد و دکتری) یکسان نبود و تفاوت‌هایی وجود داشت. پس از بررسی معناداری این تفاوت مشخص شد که در متغیرهای عوامل فردی، آگاهی از امنیت، آگاهی از حریم خصوصی، آگاهی از امنیت و حریم خصوصی و اهمیت دادن به امنیت این تفاوت معنادار است و بالاترین میزان میانگین مربوط به گروه کارشناسی بود. اما در متغیرهای اهمیت دادن به حریم خصوصی، اهمیت دادن به آگاهی و حریم خصوصی معنادار نبود.

جدول ۷. نتایج آزمون تحلیل واریانس یک‌طرفه متغیرهای پژوهش برحسب تحصیلات

متغیر	تحصیلات	میانگین	انحراف معیار	سطح معناداری لون	Fآماره	سطح معناداری آنوا
آگاهی از امنیت	کارشناسی	۸۶/۹	۵۷۱/۲	۰.۰۰۰۱	باتوجه‌به ناهمگن بودن واریانس‌ها از آزمون کروسکال والیس استفاده شد.	
	ارشد	۳۶/۷	۲۵۴/۳			
	دکتری	۲۵/۷	۲۲۷/۳			
آگاهی از حریم خصوصی	کارشناسی	۶۸/۱۰	۵۲۱/۲	۰.۰۰۰۱	باتوجه‌به ناهمگن بودن واریانس‌ها از آزمون کروسکال والیس استفاده شد.	
	ارشد	۸۸/۷	۳۰۳/۳			
	دکتری	۷۱/۷	۳۵۴/۳			
آگاهی از امنیت و حریم خصوصی	کارشناسی	۵۳/۲۰	۶۵۴/۴	۰.۰۰۰۱	باتوجه‌به ناهمگن بودن واریانس‌ها از آزمون کروسکال والیس استفاده شد.	
	ارشد	۲۴/۱۵	۱۳۳/۶			
	دکتری	۹۷/۱۴	۹۰۳/۵			
اهمیت دادن به امنیت	کارشناسی	۵۹/۱۳	۰۹۲/۲	۰.۵۶۱	باتوجه‌به اینکه توزیع متغیرها نرمال نبود از آزمون کروسکال والیس استفاده شد.	
	ارشد	۹۰/۱۲	۳۳۰/۲			
	دکتری	۷۹/۱۲	۹۳۱/۱			
اهمیت دادن به حریم خصوصی	کارشناسی	۲۷/۱۲	۵۱۲/۲	۰.۲۲۷	۰۲۰/۱	۰/۳۶۲
	ارشد	۱۲/۰۹	۴۹۲/۲			
	دکتری	۵۷/۱۱	۷۱۴/۲			
اهمیت‌دادن به آگاهی و حریم خصوصی	کارشناسی	۸۷/۲۵	۱۰۱/۴	۰/۷۰۵	۲/۷۷۱	۰/۰۶۴
	ارشد	۲۵	۲۷۳/۴			
	دکتری	۳۵/۲۴	۲۷۹/۴			
عوامل فردی	کارشناسی	۹۷/۳۳	۹۰۲/۴	۰/۶۱۱	۱۸/۰۲۹	۰/۰۰۰۱
	ارشد	۷۴/۳۰	۴۸۵/۵			
	دکتری	۵۴/۳۰	۰۸۱/۵			

طبق جدول نتایج ۸ سطح معناداری متغیرهای آگاهی از امنیت، آگاهی از حریم خصوصی، آگاهی از امنیت و حریم خصوصی و اهمیت دادن به امنیت کوچکتر از ۰/۰۵ است و نتیجه به‌دست‌آمده از نظر آماری معنی‌دار است بنابراین میانگین این سه متغیر در بین سه گروه تحصیلی متفاوت است.

جدول ۸. نتایج جدول آزمون کروسکال والیس برای متغیرهای پژوهش

متغیر	تحصیلات	میانگین	آماره کروسکال – والیس	سطح معناداری
آگاهی از امنیت	کارشناسی	۸۶/۹	۲۷۰/۵۵	۰.۰۰۰۱
	کارشناسی ارشد	۳۶/۷		
	دکتری	۲۵/۷		
آگاهی از حریم خصوصی	کارشناسی	۶۸/۱۰	۸۰۵/۶۲	۰.۰۰۰۱
	کارشناسی ارشد	۸۸/۷		
	دکتری	۷۱/۷		
آگاهی از امنیت و حریم خصوصی	کارشناسی	۵۳/۲۰	۸۲۴/۶۵	۰.۰۰۰۱
	کارشناسی ارشد	۲۴/۱۵		
	دکتری	۹۷/۱۴		
اهمیت دادن به امنیت	کارشناسی	۵۹/۱۳	۶۲۲/۱۸	۰.۰۰۰۱
	کارشناسی ارشد	۹۰/۱۲		
	دکتری	۷۹/۱۲		

پژوهش‌های زیادی (از قبیل چویی (۲۰۲۳)؛ رجب و همکاران (۲۰۲۳)؛ بونیش و باتیس (۲۰۲۱)؛ حمیدی (۱۳۹۵)؛ اسکرودر (۲۰۱۹)؛ پورهادی و همکاران (۱۴۰۱)؛ کولوچیا (۲۰۲۰)؛ ذوالفهمی و همکاران (۲۰۲۳)؛ رحیم‌خان و کادویا[1] (۲۰۲۳)؛ یسا و همکاران (۲۰۲۳)؛ البلادی و ویر (۲۰۲۰)؛ کلنامپیو (۲۰۱۸)؛ حسینی نو و مظاهری (۱۳۹۷)؛ سانی (۲۰۲۰)؛ جلالی و همکاران (۱۳۹۶)؛ آلجدانی و همکاران (۲۰۲۳)؛ کلنامپیو (۲۰۱۸)؛ یورو و همکارانش (۲۰۲۳)) در مورد متغیر جمعیت شناختی جنسیت در داخل و خارج از کشور و هم سوی با نتایج پژوهش حاضر انجام گرفت که به برخی از آن‌ها اشاره می‌شود.

چویی (۲۰۲۳) دریافت که افراد از سواد حریم خصوصی خوبی برخوردارند که در میان زنان بیشتر از مردان است و تجربیات مربوط به ویژگی‌های حریم خصوصی باعث افزایش سواد حریم خصوصی می‌شود. طبق پژوهش رحیم خان و کادویا (۲۰۲۳) تقلب‌های ضمانت وام برای زنان به طور قابل توجهی در طول همه‌گیری کاهش یافته است و کلاهبرداری‌های بازپرداخت برای مردان افزایش یافته است. همچنین یسا و همکارانش (۲۰۲۳) به این نتیجه رسیدند که زنان بیشتر احتمال داشت که درک خود را از حساسیت و مزایای مبتنی بر اعتماد تغییر دهند، زنان کمتر از مردان اطلاعات خود را در اختیار اپلیکیشن قرار می‌دهند در حالی که مردان بیشتر احتمال داشت اطلاعات را براساس درک خود از مزایا افشا کنند. آنچه در جمع‌بندی تحلیل متغیر جمعیت شناختی جنسیت می‌توان بیان کرد آن است که همانقدر که دانشجویان زن بیشتر از دانشجویان مرد، دقت و حساسیت بیشتری نسبت به مسائل امنیتی و حریم خصوصی دارند همان‌قدر هم ممکن است در معرض خطرات و تهدیدات امنیتی قرار بگیرند.

در آخر به دو پژوهشی که در مورد متغیر جمعیت‌شناختی تحصیلات انجام گرفته است و همسوی با نتایج پژوهش حاضر است اشاره کردیم و موید این مطلب است که برخلاف اینکه انتظار می‌رفت هرچه سطح تحصیلات بالاتر برود دانشجویان هم توجهشان به مسائل امنیتی و حریم خصوصی بیشتر شود اما در پژوهش حاضر نتیجه برعکس بود و اتفاقا دانشجویان لیسانس توجه بیشتری به این مسائل داشتند.

نتایج آلجدانی و همکاران (۲۰۲۳) نشان داد که در حالی که آگاهی امنیتی در میان گروه‌های جمعیتی مختلف بر اساس سطح دانش فناوری اطلاعات و سطح تحصیلات آن‌ها معنی‌دار بود. طبق پژوهش البلادی و ویر (۲۰۲۰) علاوه بر این، سطح تحصیلات تاثیر قابل توجهی بر آسیب های کاربران ندارد و میانگین لیسانس بالاتر از ارشد است.

بحث و نتیجه گیری

در دنیای به هم پیوسته امروزی بسیاری از روابط و تعاملات با دیگران مجازی است و شرایط آسانی برای تبادلات اطلاعات، اخبار، رویدادها با قابلیت نظر دادن و اشتراک گذاری اطلاعات با مخاطبان گسترده و حتی تولید محتوا را فراهم کرده‌اند. بنابراین رسانه‌های اجتماعی توجه روز افزونی را به خود جلب کرده‌اند. این حجم از تبادل اطلاعات باعث شده امنیت و حریم خصوصی کاربران در شبکه های اجتماعی به خطر بیفتد. کاربران برای مقابله با این تهدیدات باید بدانند چه عواملی بر روی امنیت و حریم خصوصی تاثیرگذار است. از میان عوامل گسترده ای که در مطالعات گذشته بیان شده، عامل فردی یکی از مهمترین عواملی است که در این پژوهش به آن پرداخته شد. حال با توجه به ضرورت موضوع، پژوهشگران در این پژوهش به بررسی « امنیت و حریم خصوصی کاربران شبکه های اجتماعی: بررسی عوامل فردی » پرداختند.

نتایج پژوهش موید این موضوع هست که دانشجویان به عنوان قشر فعال جامعه آنطور که باید از مسائل مرتبط با امنیت و حریم خصوصی آگاه نیستند و این آگاهی کمتر از حد انتظار محققان بود و علت این موضوع را شاید بتوان عدم شکل‌گیری فرهنگ استفاده از شبکه های اجتماعی و عدم توجه کافی به دستورالعمل های این نوع شبکه ها در مورد امنیت و حریم خصوصی دانست و این زنگ خطری است برای تمامی مسئولین دانشگاهی و دولتی که به فکر آموزش و آگاهی بخشی به دانشجویان باشند. برخلاف آگاهی نسبتا پایین دانشجویان، آن‌ها اهمیت زیادی برای امنیت و حریم خصوصی خود در شبکه‌های اجتماعی قائل هستند و مسلما برای تحقق بخشیدن به این موضوع و در واقع به عنوان پیش نیاز آن، آشنا بودن

[1] Rahim Khan & Kadoya

با قوانین سیاست حریم خصوصی و نحوه انجام تنظیمات امنیتی و حریم خصوصی است. به گمان محقق شاید بتوان علت این موضوع (طبق نتایج بدست آمده با اینکه دانشجویان به مسائل مرتبط به امنیت و حریم خصوصی اهمیت می‌دادند اما آگاهی آن‌ها کمتر از حد مطلوب بود) را نوعی دیدگاه سطحی نگرانه در بین جوانان امروزی دانست که بیشتر به دنبال استفاده و لذت هستند تا کسب آگاهی. مسلما برای تحقق بخشیدن به این موضوع و در واقع به عنوان پیش نیاز آن، آشنا بودن با قوانین سیاست حریم خصوصی و نحوه انجام تنظیمات امنیتی و حریم خصوصی است.

بررسی نتایج نشان داد که میزان انجام برخی از عوامل فردی (شامل مولفه‌های تجربه حمله، تغییرات موفق حریم خصوصی، دفعات بازدید، توانایی و مهارت های فناوری، سهولت درک شده) توسط دانشجویان کمتر از حد انتظار بود و در مقابل انجام برخی دیگر (شامل اعتماد به سامانه، سود درک شده، خطر درک شده، اهمیت درک شده) بیشتر از حد مطلوب بود. اما به طور کلی میانگین میزان انجام رفتارهای مربوط به عوامل فردی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی (به طور کلی) به طور معناداری کمتر از حد مطلوب بود. به عبارتی آزمودنی‌های این پژوهش در حدی که انتظار می رفت، این نوع رفتارها را انجام نمی‌دادند. چرایی اینکه چرا دانشجویان برخی از رفتارها را بیشتر از رفتارهای دیگر انجام می دهند تا حد زیادی منتج از ماهیت متفاوت این دو دسته از رفتارها است. در حالی که عوامل فردی اول بیشتر ماهیت عملی و رفتاری دارد، دسته دوم بیشتر ذهنی است و به اهمیت فرد برای این موضوع توجه می‌کند. این تحلیل تا حد زیادی موید نتایج سوال اول و دوم است که اگرچه دانشجویان برای موضوعات مرتبط با امنیت و حریم خصوصی اهمیت قائل هستند اما در عمل چندان موفق عمل نمی‌کنند.

در مورد سوال آخر که در مورد نقش متغیرهای جمعیت شناختی جنسیت و تحصیلات در امنیت و حریم خصوصی شبکه‌های اجتماعی بود می توان گفت که در تمامی متغیرها زنان همسو با بسیاری از پژوهش‌های قبلی میانگین بالاتری از آقایان داشتند. به عبارتی همواره زنان مراقبت بیشتری در مورد مسائل امنیتی در شبکه‌های اجتماعی داشته‌اند و شاید این موضوع به این برگردد که بیشتر هدف تهدید قرار می‌گیرند و آسیب‌پذیری بالاتری در این زمینه دارند. ضمن اینکه مردان معمولاً ریسک‌پذیرتر از بانوان هستند و کمتر خطرات را جدی می گیرند. عامل دیگر شاید توجه بیشتر خانم‌ها به جزئیات باشد. معمای آخر این مطالعه به نمره بالاتر دانشجویان کارشناسی در مقایسه با دو مقطع بالاتر، در همه متغیرها بر می‌گردد. واقعیت آن است جوانان دهه هشتادی که عمده دانشجویان دوره کارشناسی در این دسته قرار می‌گیرند با فناوری کاملاً اخت هستند و بسیاری از تکنیک‌های مرتبط با فضای مجازی که برای سنین بالاتر یک معمای لاینحل است برای آن‌ها جزو زندگی روزمره است. ضمن اینکه استفاده بیشتر مهارت بیشتر هم به دنبال دارد و وقت آزاد دانشجویان کارشناسی امکان استفاده بیشتر را برای آن‌ها فراهم می‌کند.

در پایان پیشنهاد می‌شود با توجه به گسترش روز افزون فناوری و استفاده هر چه بیشتر کاربران از این فضاها و نقش مهم و بسزایی که این شبکه‌ها در زندگی افراد دارند، نیاز است تا اولاً افرادی بدون پیچیدگی و با سهولت کامل تنظیمات امنیتی و حفظ حریم خصوصی در رسانه‌های جدید و سنتی را در قالب دوره‌هایی به کاربران آموزش دهند و همچنین کاربران را با خطرات و تهدیدهای بیشمار این فضاها آشنا کنند و از آنجایی که در این پژوهش زنان (نسبت به مردان) و مقطع کارشناسی (نسبت به دو مقطع بالاتر از خود) نمره بالاتری کسب کردند لذا باید بیشترین تمرکز رو بر روی این دسته از افراد گذاشت. از طرفی هم مسئولین دانشگاه به علت لزوم ضرورت این موضوع، یک واحد درسی دانشجویان را به این موضوع اختصاص دهند.

تقدیر و تشکر

بدینوسیله از همه داروان و دست‌اندرکاران مجله وزین تعامل انسان و اطلاعات، که همکاری لازم را در چاپ مقاله داشتند، صمیمانه متشکریم.

مشارکت نویسندگان

نویسنده اول: تهیه و آماده‌سازی نمونه‌ها، انجام آزمایش و گردآوری داده‌ها، انجام محاسبات، تجزیه و تحلیل آماری داده‌ها، تحلیل و تفسیر اطلاعات و نتایج، تهیه پیشنویس مقاله.

نویسنده دوم: استاد راهنمای پایان‌نامه، طراحی پژوهش، نظارت بر مراحل انجام پژوهش.

نویسنده سوم: استاد مشاور پایان‌نامه، مشارکت در طراحی پژوهش، نظارت بر پژوهش، اصلاح، مطالعه و نهایی‌سازی مقاله.

تعارض منافع

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

حامی مالی

حمایت مالی از این پژوهش از طرف دانشگاه بیرجند، دانشکده علوم تربیتی و روانشناسی در قالب پژوهانهٔ پایان‌نامه دانشجویی نویسنده اول و همچنین پژوهانهٔ برای سایر نویسندگان انجام شده است.

سپاسگزاری

از معاونت محترم پژوهشی دانشگاه بیرجند به خاطر حمایت مالی و معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود. از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

منابع

احسانی‌فر، محمد؛ رضوانیان، محمد (۱۳۹۶). نقش رفتار کاربران در احساس امنیت شبکه های اجتماعی.*کنفرانس سالانه پژوهش در علوم انسانی و مطالعات اجتماعی*، تهران.

پور نقدی، بهزاد (۱۳۹۷). فرصت‌ها و تهدیدهای امنیت در شبکه‌های اجتماعی مجازی برای دانشجویان. *پژوهش‌های راهبردی مسائل اجتماعی ایران*، ۱(۲)، ۷۱-۳۷.

جلالی، کیان پور؛ آقابابایی، مسعود(۱۳۹۶). تبیین جامعه‌شناختی مدیریت حریم شخصی کاربران جوان فیس‌بوک شهر اصفهان. *پژوهش‌های راهبردی مسائل اجتماعی ایران*، ۱ (۶)، ۶۱-۲۷.

حسین‌پور جعفر؛ مصرخانی قدیر (۱۳۹۷). نقش شبکه‌های اجتماعی مجازی بر امنیت عمومی کاربران آن. *نظم و امنیت انتظامی*،۶۶ (۲)، ۶۱۱-۶۵۹.

قضاوتی، کمال‌الدین قضاوتی، نوروزی علیرضا(۱۳۹۶). مروری بر امنیت حریم خصوصی در شبکه‌های اجتماعی برخط. *امنیت فضای تولید و تبادل اطلاعات*، ۶ (۲) :۱۰۲-۸۵.

Reference

Ahmed Mahmoud Ragab, S., & Abdelmaksoud, H. (2023). Awareness of digital privacy among users of new media. *Journal of Research in the Fields of Specific Education, 9*(44), 2495-2522. https://doi.org/10.21608/jedu.2022.166154.1755**.**

Al Hasib, A. (2009). Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *9*(11), 288-93.

Alabdulatif, A., Alturise, F. (2020). Awareness of data privacy on social networks by students at Qassim University. *International Journal of Advanced Computer Research, 10*(50), 194. http://dx.doi.org/10.19101/IJACR.2020.1048094.

Alani, M. M. (2017). Android Users Privacy Awareness Survey. *International Journal of Interactive Mobile Technologies, 11*(3), 130-144.. https://doi.org/10.3991/ijim.v11i3.6605.

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences, 8*(1), 1-24. https://doi.org/10.1186/s13673-018-0128-7. (In Persian).

Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity, 3*(1), 1-19. https://doi.org/10.1186/s42400-020-00047-5.

Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., & Rodrigues, J. J. (2018). Privacy and security issues in online social networks. *Future Internet, 10*(12), 114. https://doi.org/10.3390/fi10120114. (In Persian).

Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. A. (2023). End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers. *Journal of Systems and Software, 195*, 111519. https://doi.org/10.1016/j.jss.2022.111519.

Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthc. *Journal of Multidisciplinary Healthcare, 12* (2019), 73-81. https://doi.org/10.2147/JMDH.S183275.

Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal*, *18*(1), 48-58.

Boenisch, F., Battis, V., Buchmann, N., & Poikela, M. (2021). "I Never Thought About Securing My Machine Learning Systems": A Study of Security and Privacy Awareness of Machine Learning Practitioners. In *Proceedings of Mensch und Computer 2021*, 520-546. https://doi.org/10.1145/3473856.3473869.

Choi, S. (2023). Privacy literacy on social media: Its predictors and outcomes. *International Journal of Human–Computer Interaction*, *39*(1), 217-232. https://doi.org/10.1080/10447318.2022.2041892.

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical practice and epidemiology in mental health: CP & EMH, 16*, 24. https://doi.org/10.2174%2F1745017902016010024.

Ehsanifar, M,. & Rezvanian, M. (2016). The role of users' behavior in feeling the security of social networks. *Annual Research Conference in Humanities and Social Studies*, Tehran. (In Persian).

Frik, A., Kim, J., Sanchez, J. R., & Ma, J. (2022, April). Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing System, 407*, 1-24. https://doi.org/10.1145/3491102.3517504.

Gee, D. (2016). Rethinking Security: A discussion paper. *Ammerdown Group*.

Gerber, N., Reinheimer, B., & Volkamer, M. (2018). Home sweet home? Investigating users' awareness of smart home privacy threats. *In Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*.

Ghezavati, K., & Nowrozi, A. (2016). An overview of privacy security in online social networks. *Bi-Quarterly Scientific Promotional Herald of the Security of Production Space and Information Exchange (AFTA),* 1(2), 75-126. (In Persian).

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267. https://doi.org/10.1007/s11235-017-0334-z.

Hamidi, H. (2015). Women's point of view on ethics and personal privacy in social networks. *Quarterly Journal of Ethics in Science and Technology, 11*(1), 39-50. (In Persian).

Hossein Pour, J., & Mesrkhani, Q. (2017). The role of virtual social networks on the public security of its users. *Police order and security*, *66* (2), 659-611. (In Persian).

Hosseini Senu, S. A., & Mazaheri, E. (2017). The effect of privacy, security and perceived trust on information sharing behavior in mobile social networks: the moderating role of gender. *Journal of Information Processing and Management, 93*(6), 235-213. (In Persian).

Hu, X., Hu, D., Zheng, S., Li, W., Chen, F., Shu, Z., & Wang, L. (2018). How people share digital images in social networks: a questionnaire-based study of privacy decisions and access control. *Multimedia Tools and Applications*, 77, 18163-18185**.** https://doi.org/10.1007/s11042-017-4402-x.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56-59. https://doi.org/10.1109/MC.2018.3191268.

Jafarpour Hadi Kiashari, R., Kabuli, M.H., & Shahcheraghi, A. (1401). Analyzing the effect of objective and subjective elements on the sense of "privacy" in the architectural space. *Eastern Art and Civilization, 10*(38), 17-28. (In Persian).

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157-2177. https://doi.org/10.1007/s40747-021-00409-7.

Jalali, K.pour,. & Agha Babaei, M. (2016). Sociological explanation of privacy management of young Facebook users in Isfahan city. *Strategic Researches of Iran's Social Issues, 1* (6), 27-61. (In Persian).

Kanampiu, M. (2018). *A Study of Security and Privacy in Online Social Networks Using Social Network Analysis and Human Factors Perspectives* (Doctoral dissertation, North Carolina Agricultural and Technical State University).

Khan, M. S. R., & Kadoya, Y. (2023). Who Became Victims of Financial Frauds during the COVID-19 Pandemic in Japan?. *Sustainability*, *15*(4), 2865. https://doi.org/10.3390/su15042865

Korir, M., Slade, S., Holmes, W., Héliot, Y., & Rienties, B. (2023). Investigating the dimensions of students' privacy concern in the collection, use and sharing of data for learning analytics. *Computers in human behavior reports*, *9*, 100262. https://doi.org/10.1016/j.chbr.2022.100262.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44. https://doi.org/10.1016/j.chb.2018.01.028.

Martínez-Navalón, J. G., Fernández-Fernández, M., & Alberto, F. P. (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal?. *International Entrepreneurship and Management Journal*, *19*(2), 781-803. https://doi.org/10.1007/s11365-023-00839-4.

Mittal, N. (2023). User Perceptions of Privacy and Security in Online Social Networks. *International Journal of Innovative Science and Research Technology.1*(8), 91-94.

Nawaz, N. A., Ishaq, K., Farooq, U., Khalil, A., Rasheed, S., Abid, A., & Rosdi, F. (2023). A comprehensive review of security threats and solutions for the online social networks industry. *PeerJ Computer Science*, 9, e1143. https://doi.org/10.7717/peerj-cs.1143.

Nedeljko, M., Bogataj, D., & Kaučič, B. M. (2021). The use of ICT in older adults strengthens their social network and reduces social isolation: Literature Review and Research Agenda. *IFAC-PapersOnLine, 54*(13), 645-650. https://doi.org/10.1016/j.ifacol.2021.10.524.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119.

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook. *South African Journal of Science*, *114*(5-6), 1-5. http://dx.doi.org/10.17159/sajs.2018/20170103.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870.

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). *International Journal of Sustainable Development & Planning*, *18*(1). 255-263. https://doi.org/10.18280/ijsdp.180127.

Pensa, R. G., & Di Blasi, G. (2017). A privacy self-assessment framework for online social networks. *Expert Systems with Applications*, *86*, 18-31. https://doi.org/10.1016/j.eswa.2017.05.054.

Pour Naqdi, B. (2017). Security opportunities and threats in virtual social networks for students. *Strategic Researches of Iran's Social Issues, 1*(2), 37-71. (In Persian).

Reichel, J., Peck, F., Inaba, M., Moges, B., Chawla, B. S., & Chetty, M. (2020). 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and {WhatsApp}. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 1949-1966).

Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences*, *13*(2), 1020. https://doi.org/10.3390/app13021020.

Sani, A. A. Examining Journalists'privacy Behaviour on WhatsaPP Status Updates in Kano State, nigeria. *Zaria Journal of Communication, 7*(1), 118-130.

Saura, J. R., Palacios-Marqués, D., & Ribeiro-Soriano, D. (2023). Privacy concerns in social media UGC communities: Understanding user behavior sentiments in complex networks. *Information Systems and e-Business Management*, *21*(2), 1-21. https://doi.org/10.1007/s10257-023-00631-5.

Schroeder, C. (2019). *Susceptibility to Social Engineering: Human Vulnerabilities* (Doctoral dissertation, Utica College). Utica College.

Steiert, D. (2019). *Privacy Preservation in Mobile Social Networks* (Doctoral dissertation, University of Missouri-Columbia).

Steiert, D. (2019). *Privacy Preservation in Mobile Social Networks* (Doctoral dissertation, University of Missouri-Columbia).

Tang, Y., & Ning, X. (2023). Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems*, *165*, 113881. https://doi.org/10.1016/j.dss.2022.113881.

Van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security*, *106*, 102313. https://doi.org/10.1016/j.cose.2021.102313.

Van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security*, *106*, 102313. https://doi.org/10.1016/j.cose.2021.102313.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283-297. https://doi.org/10.1016/j.chb.2017.10.007.

Wang, Q. (2020). Towards the Understanding of Private Content–Content-based Privacy Assessment and Protection in Social Networks (Doctoral dissertation, University of Kansas).

Wei, L., Gong, J., Xu, J., Abidin, N. E. Z., & Apuke, O. D. (2023). Do social media literacy skills help in combating fake news spread? Modelling the moderating role of social media literacy skills in the relationship between rational choice factors and fake news sharing behaviour. *Telematics and Informatics*, *76*, 101910. https://doi.org/10.1016/j.tele.2022.101910.

Yi, Y., Zhu, N., He, J., Jurcut, A. D., Ma, X., & Luo, Y. (2023). A privacy-dependent condition-based privacy-preserving information sharing scheme in online social networks. *Computer Communications*, *200*, 149-160.

Yisa, V. L., Anaraky, R. G., Knijnenburg, B. P., & Orji, R. (2023). Investigating Privacy Decision-

Making Processes Among Nigerian Men and Women. *Proceedings on Privacy Enhancing Technologies*, *1*, 294-308. https://doi.org/10.56553/popets-2023-0018.

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1943-1953. DOI: 10.11591/ijece.v13i2.pp1943-1953.

Zhang, Z., Jing, J., Wang, X., Choo, K. K. R., & Gupta, B. B. (2020). A crowdsourcing method for online social networks security assessment based on human-centric computing. *Human-centric Computing and Information Sciences*, *10*, 1-19. https://doi.org/10.1186/s13673-020-00230-0.

Zulfahmi, M., Elsandi, A., Apriliansyah, A., Anggreainy, M. S., Iskandar, K., & Karim, S. (2023). Privacy protection strategies on social media. *Procedia Computer Science*, *216*, 471-478. https://doi.org/10.1016/j.procs.2022.12.159.