SAIS 2024 Proceedings

Southern (SAIS)

Spring 3-16-2024

Identifying Security Vulnerabilities and Privacy Risks to Personal Identifiable Information (PII) From a Lack of Consumer Awareness to Common Cyber Threats

Andrew Sepp

Joseph Squillace

IDENTIFYING SECURITY VULNERABILITIES AND PRIVACY RISKS TO PERSONAL IDENTIFIABLE INFORMATION (PII) FROM A LACK OF CONSUMER AWARENESS TO COMMON CYBER THREATS

Andrew Sepp
Penn State University
afs6479@psu.edu

Joseph Squillace
Penn State University
Jms10943@psu.edu

ABSTRACT

As social media as an entity has grown exponentially over the past decade, so too has the individual user base comprising the social media platform across all mediums. However, despite an almost daily deluge of news identifying a new security breach, cyber theft, archive of stolen personal data, exploitative user photos or records, violation of privacy, etc., there remains almost zero concern among individual users to maintain a secure posture when interacting with the Internet, especially social media accounts: predominantly among early age adult students (e.g., college-age 18-22). The main objective of this study and the broader impact it will make to society is identification of the most common security threats college-aged students face, isolating *why* they face these threats, and *what* is causing college-age students (users) to be so laxed with their security concerns.

EXTENDED ABSTRACT

Once the research reveals *why* this phenomenon of laxed security exists, it is an equally important in this study to demonstrate how *easy* it is to exploit user vulnerabilities to steal their *Personal Identifiable Information* (PII) using easily accessible cybersecurity tools, tricks, and tactics. A study by Park and Vieraitis (2021) grounded on the routine activities theory by Cohen and Felson (1979) is the basis for our analysis. Increased accessibility of online platforms to college aged students provides offenders with opportunities for attack. The security concern will be addressed through an introduction of a training platform specifically focused on the threats and vulnerabilities identified using *Security, Education, Training, and Awareness* (SETA). By determining *what* is causing the security lapse, then identifying *what* is the training best suited to provide an increased security posture, the focused training program will be introduced to reduce individual security vulnerability and limit cyber threat exposure to themselves and the university. The inadequate security posture of students is a concern for students. The problem extends though beyond themselves and presents a major security risk to the university. Successful identification of the vulnerabilities students face, and demonstrating the weakness of the everyday technology devices and mediums they use to become an unknown cybercrime victims, will improve their defensive footprint and lower their *Cyber Risk Threat Index* (CRTI).

This study will deploy a Mixed Methods methodology. Using a qualitative survey will allow us to better understand the cyber threats faced by college-age, why users are so laxed with their security concerns when interacting with social media, and what common vulnerabilities exist that allow them to be exploited. Using the data collected and analyzed during the qualitative steps will allow us to design several training instruments to test varying training methodologies implemented to introduce security education training and awareness (security) to the students. The integration of qualitative and quantitative data will be achieved through an exploratory strategy where our findings will guide the creation of quantitative measurement tools including pre-and post-surveys, ensuring precise evaluation of student's online behavior by comparing each population through the use of t-tests. The objective output of this research highlights its intellectual merit. This research study will highlight 1) why security is not a concern to students, 2) which training is most effective when educating users on Security Education Training and Awareness, 3) which training methodology is most effective to ensure security training is maintained and utilized by students after training is complete, 4) which training method introduced provides the best security protection for students after the study has completed, and 5) the type and nature of security training best suited to be implemented (introduced) to all students at PSU to increase the overall security footprint and posture.

KEYWORDS

Cybersecurity, Security Education, Training, and Awareness (SETA), Cyber Education, Pedagogy, Consumer Privacy

REFERENCES

1. Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly*, 665-694.
2. Ajzen, I. (1991). Theory of planned behavior. *Organizational behavior & human decision processes*, *50*(2), 179-211.
3. Park, Y., & Vieraitis, L. M. (2021). Level of engagement with social networking services and fear of online victimization: The role of online victimization experiences. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(2), 38-52.
4. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 588-608.