Center for e-Learning Security Research

NSU NOVA SOUTHEASTERN UNIVERSITY
Graduate School of Computer and Information Sciences

Social Engineering & Web Authentication: An Assessment of Personal Identifiable Information (PII) Found in Social Networking Tools (SNTs)

Daira Vargas – Advisor: Dr. Yair Levy

RESEARCH PROBLEM

The research problem that this study will address is the public availability of personal identifiable information (PII) on social networking tools (SNTs), such as Facebook®. Rabkin (2006) stated that SNTs allow users to expose information about themselves, such as their educational background, age, birthday, friends, mother's maiden name, first pet's name, and favorite food via their personal profiles. This information is also known as personal identifiable information (PII).

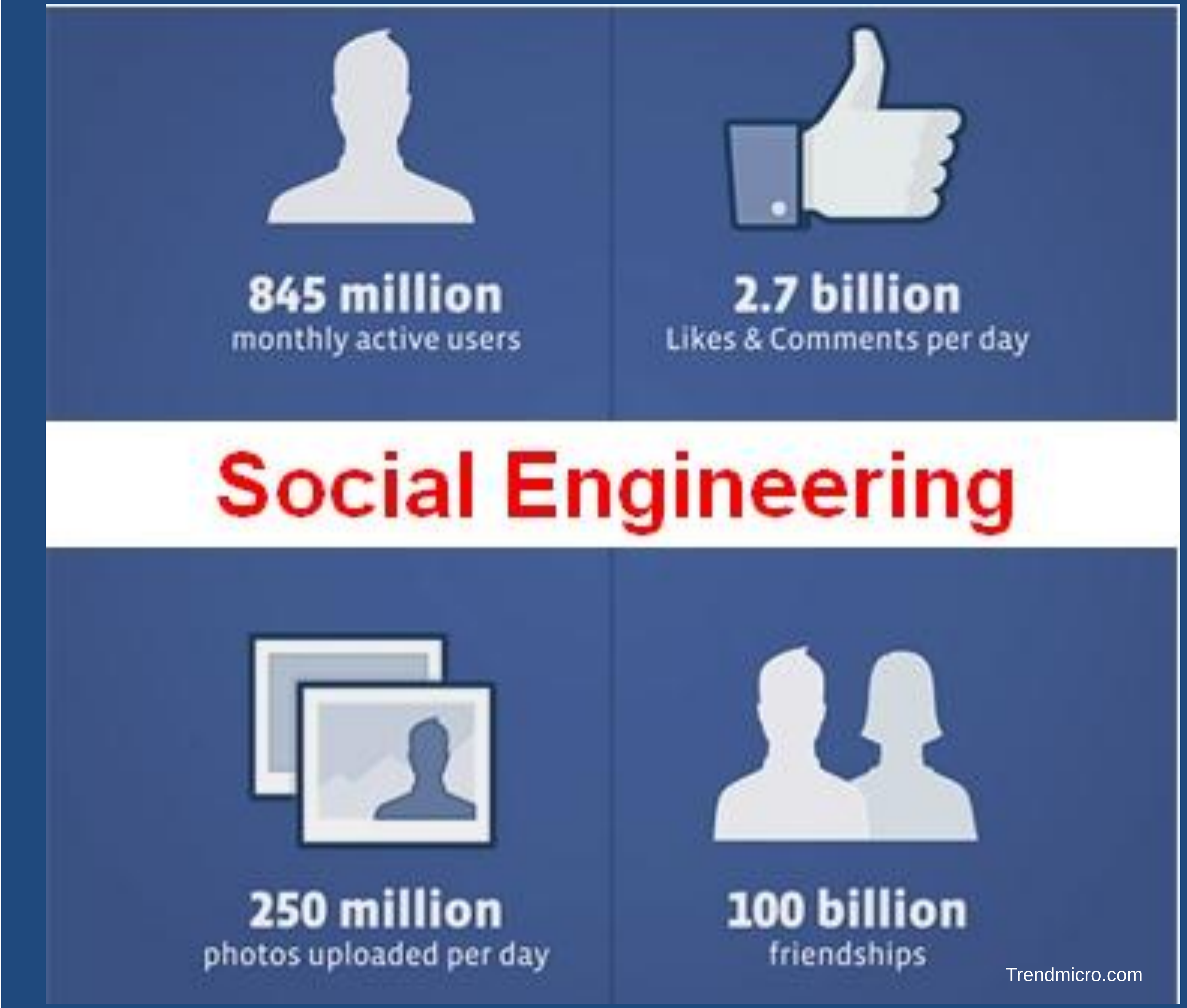
Social engineering is a technique used by hackers or other attackers to gain access to seemingly secure systems through obtaining the needed information (for example, a username and password) from a person rather than breaking into the system through electronic or algorithmic techniques (Bailey, Orgill, Orgill, & Romney, 2004).

Once an identity is compromised, the person with malicious intent can sabotage a user's online records, cancel accounts, and/or collect more personal information to create a personal profile of the victim. Thus, it appears that research to investigate PII, as it pertains to Web authentication, is highly needed.

METHODOLOGY

The goal of this proposed research is to perform an exploratory study with the objective of identifying frequently asked challenge questions and identifying PII by empirical evidences collected based on 100 accounts explored on Facebook®.

This proposed research will present an assessment of challenge questions used by the three national credit bureaus in the United States (TransUnion, Experian, & Equifax) and will examine the extent to which the potential answers can be found on Facebook® using social engineering techniques.



Trendmicro.com

REFERENCES

Bailey, M. G., Orgill, G. L., Orgill, P.M., & Romney, G. W. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information Technology Education, USA, 177-180.

Oltmann, S. M. (2010). Katz out of the bag: The broader privacy ramifications of using Facebook. *The American Society for Information Science & Technology (ASIST), 47*(1), 1-4.

Rabkin, A. (2008). Personal knowledge questions for fallback authentication: security questions in the era of Facebook. *Symposium on Usable Privacy and Security (SOUPS)*, 13-23.

RESEARCH GOALS

- What are the top 10 most frequently asked challenge questions used by the three National Credit Bureaus to authenticate individuals via the Web?
- What PII is shared by users on SNTs that would provide answers to the 10 most frequently asked challenge questions?
- Do answers to the challenge questions (PII) found on SNTs differ based on gender, age, academic level (undergraduate/graduate), number of friends, place of employment, hometown, and family listing?
- What is the ranking of the most frequently asked challenge questions in terms of available PII found on SNTs, such as Facebook®?

By identifying the top 10 most frequently asked challenge questions used by the three National Credit Bureaus to authenticate individuals via the Web, this proposed study will be able to determine which challenge questions are popular and identify any trends. According to Barnes (2006) and Grimmelmann (2009), some scholars have claimed that Facebook® users must not care about privacy since they share intimate details and personally identifiable information (Oltmann, 2010). Oltmann (2010) stated that more and more data may be publicly or semi-publicly available to be viewed, traded, bought, and sold as society's expectations of privacy decreases.