C3 Discriminating Hacker Techniques by Individual Differences and Techniques of Neutralization

Gregory Bowen, University of Alabama, 4120 Ashington Drive, Birmingham, AL 35242; and Kathryn C. Seigfried-Spellar, PhD*, Purdue University, Computer and Information Technology, 401 N Grant Street, West Lafayette, IN 47907*

After attending this presentation, attendees will better understand the different hacker tools used to commit cyber attacks as well as their relationship to individual differences and techniques of neutralization.

This presentation will impact the forensic science community by being the first study to assess the relationship between hacker tools, individual differences, and techniques of neutralization.

According to Paganini, the top five cyber security threats are: injection vulnerabilities, buffer overflows, sensitive data exposure, broken authentication and session management flaws, and security misconfiguration.[1] In addition, Symantec reported an increase in "trojanized" software updates, malware, ransomware, and social media scams in 2014; in fact, there were 317 million new forms of malicious software created this past year.[2] It is clear that escalating cyber threats and vulnerabilities are a serious concern for both small and large organizations, as well as the private sector and general public.

The term hacking has evolved over the years, but in general it refers to the use of a computer to gain unauthorized access to information systems or to someone who exploits the vulnerabilities of computer networks.[3] Nonetheless, computer crimes are similar to other types of crimes, such as homicide, in that the same crime (e.g., unauthorized access) can be committed, using different tools (e.g., password cracking, sniffing), by offenders with different techniques of neutralization (e.g., denial of injury, denial of responsibility); however, the traditional focus on cybersecurity has been on the creation of better tools, rather than understanding from whom one is being protected.[4-6]

Overall, there are a variety of hacking techniques or tools; however, it is unknown whether individuals are more likely to use multiple hacking techniques (i.e., a generalist) or if they tend to focus on a specific method or tool (i.e., a specialist). In addition, it is unknown whether there is a relationship between individual differences and techniques of neutralization for the different hacking tools/techniques. Thus, the current study will be the first to assess the relationship between individual differences and the types of tools (e.g., a Distributed Denial of Service (DDoS) attack) used by computer hackers along with differences in neutralization (e.g., denial of injury).

This study will be conducted using an anonymous, internet-based survey created in Qualtrics, and respondents will be solicited from Amazon's® Mechanical Turk. Research studies have shown Mechanical Turk may be used to obtain high-quality data inexpensively and rapidly from a diverse participant pool and provides better generalizability than snowball sampling procedures.[7] The survey will assess the prevalence of current tools used to administer various cyber attacks (e.g., DDoS, password cracking tools). In addition, this survey will measure the respondents' personality characteristics and techniques of neutralization.

The results and future implications of the study's findings will be discussed.

Reference(s):

1. Paganini P. (2015, July 2). *The Top Five Cyber Security Vulnerabilities*. Retrieved from resources.infosecinstitute.com.
2. Symantec. (2015). *Internet Security Threat Report* (Vol. 20). Retrieved from symantec.com.
3. Holt T.J., Bossler A.M., Seigfried-Spellar K.C. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge.
4. Rogers M., Seigfried K., Tidke K. (2006). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation*, 3, 116-120.
5. Seigfried-Spellar K.C., O'Quinn C., Treadway K. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour & Information Technology*. 34(5), 533-542.
6. Seigfried-Spellar K.C., Treadway K.N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, 35(10), 782-803.
7. Buhrmester M., Kwang T., Gosling S.D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality data? *Perspectives on Psychological Science*, 6(1), 3-5.

Hackers, Personality, Individual Differences

*Presenting Author