Cyberpsychology, Behavior, and Social Networking
Volume 17, Number 3, 2014
© Mary Ann Liebert, Inc.
DOI: 10.1089/cyber.2014.1502

Editorial

The Role of Psychology in Enhancing Cybersecurity

Brenda K. Wiederhold, PhD, MBA, BCB, BCN

With 70% of the world's total population projected to have access to the Internet by 2017, compared to 33% in 2011,[1] the human factor remains security's weakest link in cyberspace.[2] Psychology, through its insight into human nature, has a crucial role to play in mitigating this risk.[2] The shift of focus from technology to psychology is logical because even the most sophisticated security systems remain incapable of preventing people from falling victim to social engineering, or risking financial and social loss to a false promise of payoff. It is also necessary because of the high cost of cybercrime on societies, governments, and individuals.

A study published by Norton Internet Security estimated that cybercrimes cost individuals,[3] corporations, and governments more than $100 billion in 2012 alone. It also highlighted a 200% rise in cost per victim compared to the previous year.[3] The impact of cybercrime, however, goes beyond financial detriment; researchers found that victims often experience symptoms similar to those of post-traumatic stress disorder (PTSD). Others have found a high risk of secondary victimization among people close to victims.[4]

Individuals are at a psychological disadvantage when faced with cybercrime.[5] They are often not presented with sufficient information to make optimal decisions in privacy sensitive situations.[5] Calculated under this bounded rationality, estimates of risk-versus-payoff parameters are skewed.[5,6] But even in cases when sufficient information is available, individuals, enticed by prospects of immediate gratification, and under the influence of optimism bias, tend to fall victim of hyperbolic discounting, and assign lower risk values to privacy decisions.[7]

Using their understanding of human behavior in cyberspace, psychologists can introduce cultural and behavioral shifts toward higher security on both the individual and the collective levels through:

1. Understanding the behavioral economics governing people's perception of risk and reward, in light of the aforementioned cognitive limitations. Also, identifying social situations in which individuals demonstrate a higher tendency to discount the risk of sharing private information. For example, a study found that people are more likely to reveal personal and confidential information in less formal settings, such as casual conversation or on social networks.[8]
2. Identifying patterns of criminal and malicious activities through observing deviations from normative behavior, and interacting with technology providers to develop security systems capable of detecting such activities, taking into consideration the psychological distortion influencing privacy decisions.[9]
3. Advising legislators and steering groups on the psychological and the social impact of cybercrime in order to elevate legislation to a level comparable to that of nonvirtual crimes. A study across 64 countries has identified that fragment legislation (i.e., legislation variance across countries) is one of the major factors that hinder fighting cybercrime.[10]
4. Raising public awareness of cybersecurity risks to adjust people's perception and, subsequently, their behavior toward privacy. It is essential that psychologists reach out beyond labs and journals to communicate with the public through mainstream media and social networks.
5. Understanding the impact of cybercrime on victims' behavior throughout the stages of victimization. Researchers found that victims of cybercrime go through three stages upon engaging with fraudulent interactions, similar to those associated with rites of passage: preliminal (separation), liminal (transition), and postliminal (incorporation).[11] Psychologists should understand the symptoms and outputs of each phase in order to optimize and keep treatment and therapy practices up-to-date.

In her testimony to a congressional subcommittee about the role psychologists play in preventing cyber-attacks, human factor psychologist Anita D'Amico said, ''As researchers and educators, we must address all the many different roles that we humans play in cybersecurity, beyond just the security practitioner who administers firewalls, tunes intrusion detection systems and monitors networks. We must also educate the software developer, lawyer, policymaker and all of us users who are unwitting accomplices of the attacker.''[12]

References

1. UNODC. (2013) Comprehensive study on cybercrime. www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed Dec. 16, 2013).
2. MIT. (2013) Cyber security and human psychology. http://cybersecurity.mit.edu/2013/11/cyber-security-and-human-psychology (accessed Dec. 15, 2013).
3. Symantec. (2013) 2012 Norton cyber crime report. http://now-static.norton.com/now/en/pu/images/Promotions/2013/PDFs/NCR%20-%20%20Mobile%20-%20Europe%20FINAL%20FINAL.pdf (accessed Dec. 17, 2013).

4. Kirwan G, Power A. (2011) *The psychology of cyber crime*. Pennsylvania: IGI Global Press.
5. Acquisti A. (2004) Privacy in electronic commerce and economics of immediate gratification. In *5th ACM Conference on Electronic Commerce.* New York: ACM Press, pp. 21–29.
6. Baddeley M. (2011) *Information security: lessons from behavioural economics*. Cambridge: Cambridge University.
7. Acquisti A. (2004) Privacy in electronic commerce and economics of immediate gratification. In *5th ACM Conference on Electronic Commerce.* New York: ACM Press, pp. 21–29.
8. John LK, Acquisti A, Loewenstein G. Strangers on a plane: context-dependent willingness to divulge sensitive information. Journal of Consumer Research 2011; 37: 858–873.
9. Morewedge CK, Gilbert TD, Wilson TD. The least likely of times how remembering the past biases forecasts of the future. Psychological Science 2005; 16:626–630.
10. UNODC. (2013) Comprehensive study on cybercrime. www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed Dec. 16, 2013).
11. Burgard A, Schlembach C. Frames of fraud: a qualitative analysis of the structure and process of victimization on the Internet. International Journal of Cyber Criminology 2013; 7:112–124.
12. Mumford G. (2009) Preventing cyber attacks. www.apa.org/monitor/2009/09/cyber-attacks.aspx (Dec. 17, 2013).

Brenda K. Wiederhold
Editor-in-Chief