Victim Precipitation in Cyber Victimization & Potential Remedies

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 201S: Cybersecurity & Social Science, Professor Trinity Woodbury

February 18, 2025

Assignment Question:

Apply the phrase, "Victim Precipitation to Cyber Victimization."

What is Victim Precipitation in Cyber Victimization?

A user's actions (or lack of security awareness) contribute to their demise and victimization in a cyberattack (Wagen & Pieters, 2020; Petherick, 2017). Active precipitation occurs when a user unknowingly engages in risky behavior that invites an attack. Examples may include clicking on phishing links in emails, downloading malicious attachments, using weak passwords, or reusing the same credentials across multiple website accounts. Passive precipitation is when a user's lack of awareness or negligence makes them vulnerable and more straightforward to target for hostile threats. Examples may include failure to update software or leaving vulnerabilities open on one's computer, using out-of-date or obsolete forms of authentication instead of multi-factor authentication (MFA) when available, and ignoring security warning notifications and pop-ups from a device from various applications (e.g., antivirus, system alerts). Several real-world cyber incidents where victim precipitation played a role in cyber victimization include the Colonial Pipeline Ransomware Attack (2021), the 2017 Equifax Data Breach, the 2013 Target Data Breach, and the 2020 Twitter Bitcoin Scam.

How does a person proactively minimize or reduce the possibility of victim precipitation in cybersecurity?

First, intentional cybersecurity education from the end user. Technology is constantly growing and fast: the end-users must self-educate themselves using the internet by researching the latest cybersecurity trends from trusted media outlets. End-users can also sign up for webinars or online courses from seasoned professionals and watch YouTube videos about their most used or favorite applications to learn how to use them better and secure their data. Also, self-paced education and research using the abovementioned options help people use more caution and prudence with unknown emails, links, attachments, and phone calls from social engineering threats. Some end users may have access to free content, online resources, and seasoned professionals at their place of employment. Their IT and HR departments are the point of contacts for help connecting to or locating those options. Lastly, those more advanced in understanding technology and cybercrime can responsibly experiment with penetration testing tools on their own ad hoc/virtual machines from Trend Micro to conduct various tests like Phishing Campaigns (e.g., Phish Insights).

Second, using strong authentication methods and security protocols (i.e., MFA, password managers). Popular and safe MFAs are Google and Microsoft Authenticators, which provide software tokens, and YubiKeys, providing hardware token solutions. Using Long and complicated passwords for important accounts along with using a password manager—like LastPass, Proton Pass, and Bitwarden—to keep track of them all without having to write them down or memorize each. Using the most up-to-date security protocols: changing one's SOHO default router credentials while updating the router's firmware to use WPA3 instead of WPA2 (anything less than

WPA2 is inviting nefarious trouble). For advanced end-users, blocking vulnerable or unused ports like Telnet (Port 23) or HTTP (Port 80) and primarily using HTTPS (Port 443) for internet browsing is beneficial too.

Lastly, conducting routine, consistent, and preferably automatic software updates. Large, name-brand corporations provide routine patches and updates to their systems and notify users in advance of these events. NVIDIA's patches come about once or twice a month, either at the beginning or the end of it. Microsoft usually pushes its patches and updates on the second Tuesday of each month (i.e., Patch Tuesday). Utility applications like CCleaner can help streamline the updating process by conducting routine scans for the end user and then populating applications that need updates. If utility applications cannot download and install the most recent firmware, the end user can directly visit the manufacturer's website to do this themselves. From my personal experience, I have done this a lot within the past several months for my Intel Processing Chip, NVIDIA GPU, and updating my Bios: there lots of performance power output issues affecting the latest Intel chips, potentially drawing on too much power and frying the circuitry.

References

Petherick, W. (2017). Victim Precipitation: Why we need to Expand Upon the Theory. *Foresic Research & Criminology International Journal, Vo.l. 5*, 262-264.

Wagen, W. v., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17(4)*, 480-497. Retrieved from https://journals.sagepub.com/doi/full/10.1177/1477370818812016