Cyber Fraud, Scam and Cons—Vulnerabilities

AMU

Samuel Speed, Jr.

SCMT537 Computer Crimes

January 23, 2021

Cyber fraud is a type of crime committed via a computer to deceive another person's data accessible through the internet. Cyber fraud is the leading type of fraud; individuals and firms are supposed to protect themselves from attackers (Drew, 2018). Cybercrime is an international threat and has been expanding rapidly throughout the twenty-first century, giving room for fraudsters to differently hack personal and financial information. Fraudsters or cons gather the information for personal gain when using the acquired data or financial information to fund terrorism, another leading threat in the security sector. Some examples of severe cyber fraud crimes and cons include Home Depot's hacking, a leading retailer company in the United States, where fraudsters hacked fifty-six million customer credit cards in 2014 via cybercrime. In 2015, another case occurred in the Office of Personnel Management, United States. A China fraudster stole over twenty million personal information, including fingerprints, posing a threat to its security. Fraud cost the United Kingdom £190 billion in the year 2017, following the Annual Fraud Indicator. Reports from the Office for National Statistics (ONS) show that fraudulent crimes have cost the government vast masses of money loss, cyber fraud being the leading crime.

However, one can protect themselves from cyber fraud in different ways. Fraudsters usually hack personal information through phishing emails and viruses; therefore, it is vital for one not to log in or provide personal information, including bank details, in an email that provides such a link. The key to avoiding this crime is understanding your bank well and analyzing the related bodies that would ask for such information (Sun et al., 2018). No matter how legitimate the email or phone call sounds, one should first confirm with the bank before providing any information.

Another way of protecting yourself from cons include destroying or discarding any traces of personal and financial data. It is vital to shred any personal information provided by your bank online as fraudsters can use this information in a recycle bin to process a Card Not Present payment (CNP). Also, one should protect their computer with antivirus software to combat any fraudster contact. One should monitor their account, check credit reports and report any suspicious activity to protect themselves from cons.

A scam is simply a fraudulent act of operation to trick or cheat someone for personal gain, especially money. For instance, a bank will never ask someone about their details like credit card or social security number through the phone. Some scams include a company you have never dealt with before contacting you, whether via the telephone or face to face. One needs to go to the company's website and check their information and if it is possible to call from there to enquire if it is legitimate (Coburn et al., 2018). Scammers can use fake websites with official-looking emails to fool people. Therefore, one should ensure that the website they are visiting has a secure link and the easiest way is to check the padlock symbol from the browser.

Being rejected for a credit card, yet you have a good credit history is a scam alert—there is a chance that one is assuming your identity and using your identity for personal gain. No legitimate company will rush someone to hand over their data or decide; therefore, someone should think twice before making any decision in case of one. Scammers use the psychology of fear as a tactic to bully someone into action hence making a quick decision without enquiring. Individuals should avoid dodgy spelled emails with bad grammar because legitimate emails from major companies are always proofread and checked before sending.

Cybersecurity has faced significant threats and vulnerabilities internationally throughout the past years despite national security and awareness. How? In cybersecurity, vulnerability describes a flaw that can be manoeuvred by a cyber-attack to perform illegal operations and gain unauthorized data from a computer system (Liu et al., 2019). Vulnerabilities give room for attackers to control the system's memory, modify sensitive data, run codes, or install malware. For one to exploit the vulnerability, the attacker should have a connection to the computer system. Some of the exploitation methods include SQL injection, cross-site scripting, open-source kits, and buffer overflows.

Should vulnerabilities be publicly disclosed? Investigated vulnerabilities remain a contentious topic. Some cybersecurity researchers support disclosure, including how to manoeuvre the vulnerability. In contrast, some experts argue that direct exposure facilitates secure software and fast patching—enhancing information and application security (Subrahmanian et al., 2015). Other supporters disregard disclosure, arguing that there will be vulnerability exploitation; some believe in limited to no exposure to selected groups to reduce the exploitation risk.

There is, however, a difference between vulnerability and threat despite most cyber securities referred to as vulnerabilities. The risk is the likelihood and impact of the exploited vulnerability. When the impact and likelihood of the exploited vulnerability are minimal, then the risk is low and vice versa. Cyber attack impact ties to the Confidentiality, Integrity or Availability resource or the CIA triad. With the CIA school of thought, there are instances where typical vulnerabilities have zero risks. For example, when the exposure of an information system has no impact on an individual or organization. A vulnerability becomes exploitable when it has at least one known working attack vector. The vulnerability window is the time between the introduction of the exposure to patching.

SQL injection—a web security vulnerability gives room for the attacker to interfere with database application queries (Alwan, 2017). In general, the vulnerability allows an attacker to view information that they cannot typically retrieve—for instance, data from other users or the application's data. In most case4s, attackers steal, modify, or delete data, creating a persistent change in the application's behavior or content. In other cases, an attacker can mount an SQL injection to accommodate the back-end infrastructure, underly the server or deny a service attack. In recent years, data breach resulting from SQL injection has led to the damage of reputation; in other cases, an attacker can acquire a persistent backdoor in a company leading to long-term accommodation. Some SQL injection examples include blind SQL injection, UNION attacks, retrieving confidential data, and examining the database.

In buffer overflow, attackers exploit by overwriting a memory's application (Satish, 2017). The changes execute a path triggering file damage response and the exposition of private information. For example, an attacker can initiate an extra code creating new instructions altering the program hence gaining access to the system. In case the attacker knows the memory program layout, they can intentionally feed output the buffer cannot support, overwriting executable codes and replacing them with their own hence gaining control. Some of the buffer overflow attacks include heap and stack-based attacks.

Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) are other categories of vulnerabilities. XSS gives room for the fraudster to perform arbitrary JavaScript within the browser, whereas CSRF allows the victim to perform actions they did not intend. CSRF applies to actions the user can perform; most applications implement CSRF defences, but they leave one or two activities, creating room for exposition. CSRF is a one-way vulnerability that makes the user use HTTP requests not to retrieve the right response (Ruch et al., 2014). On the other hand, XSS is a two-way vulnerability whereby the attacker's injected script can read replies or issue recommendations.

The OS command injection also referred to as the shell injection—allows the attacker to execute the Operating System (OS) commands to the server running the application, giving room for data and application compromise. Often, the attackers leverage the vulnerability to compromise the hosting infrastructure and exploit trust relationships pivoting other systems' attacks in the organization. Some of the ways attackers inject OS command are using shell metacharacters, back sticks, and dollar characters for inline execution and command separators for Unix-based systems.

However, there are ways of preventing these vulnerabilities, including using prepared statements and following code vulnerability for SDQL injection. Preventing buffer overflows include data execution prevention and Address space randomization (ASLR). Validating number input, input containing alphanumeric characters, and validating against a whitelist prevents OS command injection attacks. Effective use of CRSF tokens prevents XSS attacks, but they do not prevent stored XSS vulnerabilities.

Penetration testing, ethical hacking, tests information technology (IT), and assets to discover the vulnerabilities an attacker may escape (Weidman, 2014). Ethical hacking is either manually operated or software automated. The process gathers target information, identifies possible vulnerabilities, exploits, and reports the findings; organizations can use ethical hacking as a security policy, employee security, and adherence compliance.

Moreover, google hacking can be used as a way of managing vulnerability. Google hacking uses search engines such as Microsoft Bing to locate vulnerability (Zhang et al., 2014). This method uses advanced search operators that find any information coincidentally exposed through misconfiguration. Security experts use chosen queries to discover subtle data to prevent exposure to the public.

**References**

Alwan, Z. S., & Younis, M. F. (2017). Detection and prevention of sql injection attack: A survey. *International Journal of Computer Science and Mobile Computing*, *6*(8), 5-17.

Coburn, A., Leverett, E., & Woo, G. (2018). *Solving cyber risk: protecting your company and society*. John Wiley & Sons.

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537-549.

Liu, S., Dibaei, M., Tai, Y., Chen, C., Zhang, J., & Xiang, Y. (2019). Cyber vulnerability intelligence for Internet of Things binary. *IEEE Transactions on Industrial Informatics*, *16*(3), 2154-2163.

Ruch, W., Martínez-Martí, M. L., Proyer, R. T., & Harzer, C. (2014). The Character Strengths Rating Form (CSRF): Development and initial assessment of a 24-item rating scale to assess character strengths. *Personality and Individual Differences*, *68*, 53-58.

Satish, P. S., & Chavan, R. K. (2017). Web browser security: different attacks detection and prevention techniques. *International Journal of Computer Applications*, *170*(9), 35-41.

Subrahmanian, V. S., Ovelgonne, M., Dumitras, T., & Prakash, B. A. (2015). The global cyber-vulnerability report.

Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45-56.

Weidman, G. (2014). *Penetration testing: a hands-on introduction to hacking*. No Starch Press.

Zhang, J., Notani, J., & Gu, G. (2014, September). Characterizing google hacking: A first large-scale quantitative study. In *International Conference on Security and Privacy in Communication Networks* (pp. 602-622). Springer, Cham.