Old Dominion University

ODU Digital Commons

Cybersecurity Undergraduate Research Showcase

2023 Fall Cybersecurity Undergraduate Research Projects

Digital Crime Prevention Is Possible

Michael Kennedy
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/covacci-undergraduateresearch

 Part of the Educational Technology Commons

Kennedy, Michael, "Digital Crime Prevention Is Possible" (2023). *Cybersecurity Undergraduate Research Showcase*. 13.
https://digitalcommons.odu.edu/covacci-undergraduateresearch/2023fall/projects/13

This Paper is brought to you for free and open access by the Undergraduate Student Events at ODU Digital Commons. It has been accepted for inclusion in Cybersecurity Undergraduate Research Showcase by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

Digital Crime Prevention is Possible

Michael Kennedy

Old Dominion University

Phil Mann

December 1, 2023

Introduction

With the digital boom continuing to grow, many online users find this as an opportunity to harm others online. I am excited to share pivotal information, statistics, and strategies to protect your digital identity. Three specific topics that I will inform you about are phishing, cyber bullying, and non-payment. These three topic points are chosen intentionally because they are common to occur to the everyday online user. Furthermore, any one of these events listed above can be life-changing for the wrong reasons. Examples of digital crimes such as phishing, non-payment/non-delivery, and cyberbullying being mitigated by efficient preventative measures are a great example that it is possible to successfully protect individuals and organizations from falling victim to online threats in the digital space.

Phishing

Phishing may be a term you may not be familiar with. However, with its continuous rise it is important to understand what it is. Phishing is a technique for attempting to acquire sensitive information, through fraudulent emails or on a web site impersonating others (NIST). “80% of reported cybercrimes are generally attributed to phishing attacks in the technology sector.” (Palatty) There are many different methods of phishing, but they all revolve around an attacker sending fraudulent communications enticing a citizen to fall victim. The impersonators look to

extract vital private information like social security numbers, bank details, and device access. “50% of American internet users had their accounts breached in 2021.” (Griffith) This is an extremely high rate and a concern for individuals acting out unethical attacks on other citizens online. A few tips to prevent yourself from falling victim to phishing include frequent system updates, to never share your password, and to analyze the email or message to point out red flags like typos (OCC).

Cyberbullying

Cyberbullying is another issue in the digital realm. Cyberbullying is when one is bullied and harassed over digital devices like cell phones, computers, and tablets. (SB) More than 59% of US teenagers have experienced bullying or harassment online. Many teenagers have had their online experience ruined by unacceptable actions by others. Students are almost twice as likely to attempt suicide if they have been cyberbullied (Vojinovic). I am more than happy to show you indications a loved one possibly would show if they were a victim of cyberbullying. A few of the signs are them becoming upset, sad, or angry during or after being online or using their phone, withdrawing from family or friends, and signs of depression or sadness (ADL). Being attentive online and around loved ones can save lives and prevent cyberbullying from occurring. There are many steps that one should implement to keep themselves secure from cyberbullying like setting appropriate settings for social media accounts. Setting up privacy settings will limit the communication from a cyberbully. The next step is refusing to respond to cyberbullies and to keep receipts of the messages for when reporting the actions. Most importantly, contact law enforcement if you feel threatened (Gordon).

Non-payment

The second most common type of cybercrime is non-payment and non-delivery. The study

stated that it was reported 51,679 times in 2022 (Fong). Non-payment/non-delivery is when you don't get paid if you ship an item, you sold or you don't get an item you paid for (Griffith). Purchasing a product or service and not receiving what you are owed should never happen online. Here are a few different methods to protect yourself from being scammed. First, never click on links or attachments in unsolicited emails or on social media, regardless of how amazing the offer may be. If an ad looks too good to be true, then it likely is. Also, conduct brief research on the alleged associated retailer directly (DV).

Relevancy

Being involved in an online attack can be time consuming, costly, and extremely frustrating. Hackers tend to obtain access to personal documents, photos, access to bank accounts to take as much money as possible. The purpose behind an attacker phishing using their email is "to steal money, gain access to sensitive data and login information." (Cisco) Private photos, messages, and birth certificates etc. can be in the wrong hands from clicking on a deceiving link. Unfortunately, some users online take their personal problems out of strangers. The extreme impact cyberbullies have on their victims is not to be taken lightly like depression. Lastly, depending on which platform you buy a service or good from they will not refund you of your transaction. Your hard-earned money would be gone in an instant from not verifying the authenticity of the vendor. The average time to solve a cybercrime is a little over 6 hours, my goal is to also save you time and the headache.

Prevention

In order to halt cybercrime from negatively affecting you, then you need to briefly understand what you are facing. Educating yourself is step one, to set up proper parameters to keep your digital presence safe. A helpful site is "Statistaz" (www.statista.com); it's another great option

to expand your knowledge to bridge the gap between being unfamiliar with cybercrime and being aware. Statistaz is a database that provides statistics, relevant reports, and insights about digital crime. This resource provides a major opportunity to expand users' knowledge which is extremely beneficial. Surprisingly, I learned that extortion was a top four most common reported cybercrime in 2022. More recognition of digital crimes will make it more difficult for attackers to complete their attacks or illegal acts.

Who to contact if this occurs

There are many different types of resources available to assist you if you unfortunately were a victim from a digital crime. I will highlight a few major sources to help you or a loved one if there was an illegal issue occurring online. First resource that I recommend is the Internet Crime Complaint Center (www.ic3.gov). There are multiple services provided on the site such as filing a complaint, statistics, and information for digital awareness. Next, your local authorities can also provide support to alleviate your online issues. The Department of Justice recommends that you "report the issue to appropriate law enforcement and investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement." (DOJ)

Conclusion

Overall, when exploring the internet no one wants to be harassed, hustled for money, or scammed. I look forward to implementing the strategies discussed to safeguard my information and identity while online. There are many different methods to protect your online experience and data. Proven and appropriate steps must be taken to deter an attack from successfully completing their scheme to harm you.

Work Cited

(ASPA). “What Is Cyberbullying.” *StopBullying.Gov*, 1 Aug. 2023, www.stopbullying.gov/cyberbullying/what-is-it.

“Cyberbullying Warning Signs.” *ADL*, www.adl.org/resources/tools-and strategies/cyberbullying-warning-signs. Accessed 1 Dec. 2023.

“Diamond Valley FCU Blog | Diamond Valley FCU.” *Www.diamondvalleyfcu.org*, www.diamondvalleyfcu.org/blog/don%E2%80%99t-get-caught-non-delivery-scam. Accessed 1 Dec. 2023.

“Facts about Cyberbullying.” *Facts About Cyberbullying | Annapolis, MD*, www.annapolis.gov/908/Facts-About Cyberbullying#:~:text=Nearly%2042%25%20of%20kids%20have,had%20their%20feeli n gs%20hurt%20online. Accessed 1 Dec. 2023.

Fong, Jimmy. “Global Cybercrime Report: Which Countries Are Most at Risk in 2023?” *SEON*, 4 May 2023, seon.io/resources/global-cybercrime report/#:~:text=Non%2DPayment%2FNon%2DDelivery,they%20are%20not%20necessari ly%20linked.

Gordon, Sherri. “10 Tips for Preventing Cyberbullying in Your Teen’s Life.” *Verywell Family*, Verywell Family, 22 July 2022, www.verywellfamily.com/how-to-prevent cyberbullying-5113808.

Griffith, Eric. “Non-Payment/Non-Delivery Is the Top Cybercrime, Not Data Breaches.” *PCMAG*, PCMag, 25 Oct. 2018, www.pcmag.com/news/non-paymentnon-delivery-is-the

top-cybercrime-not-data-breaches

“Internet Crime Complaint Center (IC3).” *Internet Crime Complaint Center(IC3) | Home Page*, www.ic3.gov/. Accessed 1 Dec. 2023.

NIST. “Phishing - Glossary | CSRC.” *Nist.gov*, 2015, csrc.nist.gov/glossary/term/phishing.

Palatty, Nivedita James. “90+ Cyber Crime Statistics 2023: Cost, Industries & Trends.” *Astra Security Blog*, 26 Oct. 2023, www.getastra.com/blog/security-audit/cyber-crime statistics/#:~:text=The%20global%20annual%20cost%20of,%248%20trillion%20annuall y %20in%202023.&text=Cybercrime%20Magazine-,80%25%20of%20reported%20cyber%20crimes%20are%20generally%20attributed%20t o %20phishing,4.91%20million%20in%20breach%20costs.

Palatty, Nivedita James. “90+ Cyber Crime Statistics 2023: Cost, Industries & Trends.” *Astra Security Blog*, 26 Oct. 2023, www.getastra.com/blog/security-audit/cyber-crime statistics/#:~:text=Top%20Cyber%20Crime%20Statistics%202023,-The%20global%20annual&text=Cybercrime%20Magazine-,80%25%20of%20reported%20cyber%20crimes%20are%20generally%20attributed%20t o %20phishing,4.91%20million%20in%20breach%20costs.

“Phishing Attack Prevention: How to Identify & Avoid Phishing Scams.” *Www.occ.gov*, 6 Apr. 2019, www.occ.gov/topics/consumers-and-communities/consumer protection/fraud-resources/phishing-attack-prevention.html#howtoprotect.

"Reporting Computer, Internet-Related, or Intellectual Property Crime." *Criminal Division*, 11 Aug. 2023, www.justice.gov/criminal/criminal-ccips/reporting-computer-internet related-or-intellectual-property crime#:~:text=Internet%2Drelated%20crime%2C%20like%20any,offices%20of%20federal%20law%20enforcement.

"U.S. Most Frequently Reported Cyber Crime by Number of Victims 2022." *Statista*, 29 Aug. 2023, www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime us/.

Vojinovic, Ivana. "Heart-Breaking Cyberbullying Statistics for 2023." *DataProt*, 5 May 2023, dataprot.net/statistics/cyberbullying-statistics/.

"What Is Phishing? Examples and Phishing Quiz." *Cisco*, Cisco, 9 Nov. 2023, www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html.