Cyber Crime Journal: Cyber Bullying

Module 1 : Cyberbullying

Cyberbullying is bullying that takes place over the internet, apps, social media, etc. It consists of sending hateful, disrespectful, rude or untrue information about someone else to that person(s) or other people.

In the state of Maryland, if you are caught cyberbullying and sent to court, by Grace’s Law, you can be sentenced to prison for up to 3 years or fined up to a maximum of $10,000. There is no set federal law when dealing with cyberbullying, thus most states (44) have their own sets of laws regarding cyberbullying. This law was altered and established in 2013, as a teen named Grace McComas committed suicide from being cyberbullied by her neighbor. This is important as many other teens, kids and young adults are cyberbullied.

In 2021, a 12-year-old child named Jaylen White was being cyberbullied. He had disconnected from social media but someone the bully was still hacking his PlayStation Network, Netflix and YouTube showing threatening messages that White should commit suicide and if he did the cyberbullying would end. Ultimately, the bully actually apologized saying his “mother had caught him” and that he would stop. After that the bullying had ceased and nothing happened since. White’s mother still wants to find out who the bully was and hold that person accountable.

Personally, I believe that story is so sad. Nobody really knows how cyberbullying can affect someone unless they go through it. It is just another form of bullying and can cause lifelong mental health issues for that person. It is sad that a 12-year old kid had to go through that situation but I am glad that the cyberbullying stopped. I agree with his mother, I too would want to know who did this and they should be held responsible for their actions.

SOURCES:

*Bullying Laws in Maryland*. (2019). Cyberbullying Research Center. <https://cyberbullying.org/bullying-laws/maryland>

Sbraccia, S. (2019, July 1). *Cyberbullying of Wilson 6th grader abruptly stops after possible hacker says mom ‘told me to apologize.’* CBS 17. <https://www.cbs17.com/news/investigators/cyberbullying-of-wilson-6th-grader-abruptly-stops-after-possible-hacker-says-mom-told-me-to-apologize/>

Cyber Crime Journal: Cyber Crime Laws

Module 1: Cyber Crime Laws

The Health Insurance Portability and Accountability Act (HIPAA) (1996) provides protections for individuals and their health histories and information. This law gives individuals privacy and more control over their own health and well-being. Violating HIPAA would mean giving out a patient’s personal health information.

The crime this law targets is patient privacy. If you were to give out a patient’s information or disregard their personal wishes for their medical appointments, this could potential go against the person’s individual safety and privacy.

Violations against Health Insurance Portability and Accountability Act (HIPAA) (1996) can lead to very serious punishments. If you violated HIPAA in a very profound way, the minimum fine amount is $50,000. The maximum fine amount is $250,000. For healthcare providers (doctors, nurses, etc.) they can lose their licensing and never work in health ever again.

In November of 2021, a physical therapy healthcare center was breached and during the breach, employees and patients of the clinic were notified that their personal information may have also been breached. This event was logged into the official HIPAA Breach Page, as the information from these clients and professionals may have lost privacy of their financial accounts. Although no real penalties were issued, those affected were offered free credit monitoring, at the event that their financials were in danger. Personally, I would be scared because these people did not do anything to put them in this type of danger. They routinely put their trust in this clinic but their financials and other important private information may be at risk, and once they are breached it is very difficult to bounce back and even possibly get back to normal.

**SOURCES:**

*Data breach at US healthcare provider Viverant PT impacts more than 6,500 patients*. (2021). The Daily Swing. <https://portswigger.net/daily-swig/data-breach-at-us-healthcare-provider-viverant-pt-impacts-more-than-6-500-patients>

*Summary of the HIPAA Privacy Rule*. (2017). US Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

Week 3 Journal : Cyber Stalking and Predators

Module 2 : Cyber Stalking and Predators

Cyber stalking is using the internet, social media or technology to stalk someone online. It is a branch of cyber bullying but more persistent and methodical. Although the receiving end may express they wish the stalker to stop, this does not stop this person. It can lead to violence, feelings of distress, stress, anxiety, etc.

For the most part, cyberstalking is a penalty at most local levels and on a federal level. Depending on the severity of the circumstance, cyber stalking can lead to one year in prison to up to a life sentence. In Maryland, if you are deemed guilty of cyber stalking, you can be granted a $10,000 fine and up to three years in prison. If you cause a minor to commit suicide, it can be up to 10 years in prison and the $10,000 fine.

In February of 2020, a 19-year-old man harassed students from his local high school as well as multiple other places online for six years. Specifically, he harassed one girl in which he threatened to kill her and bomb the school. He was finally caught after he had sent multiple threatening messages as well as hacked into multiple databases. Like the school’s grading system and online accounts of the victims and their families. After being caught, police officers discovered he had also hacked into multiple government and private websites. He faces a ten-year sentence if convicted.

Personally, I believe he deserved more sentencing. This is a really crazy story and if I were the victim or their family, I would be worried for my safety even after this situation resolved. Things like this can scar and cause individuals trauma for the rest of their lives.

SOURCES:

*US Teen Arrested Over Alleged Swatting and Cyberstalking*. (2020, February 18). Info Security Group. <https://www.infosecurity-magazine.com/news/us-teen-swatting-cyberstalking/>

*What Is Cyberstalking?* (2021). Verywellmind. <https://www.verywellmind.com/what-is-cyberstalking-5181466>

Week 4 Journal : Cyber Terrorism

Module 3 : Cyber Terrorism

Cyber Terrorism is where individuals and groups of people abuse the powers of computers and technology in order to spread fear and gain power over a government and/or its people. Many cyber terroristic attacks are done for money and power, each case varying in details.

Cyber attacks are where it can be incidental, these attacks are often because the individual or group wants to gain a specific amount of money, information, or vandalize the data. These differ from cyber terrorism as these attacks can be unplanned and just a random account or individual is being targeted. Cyber terrorism ( I believe) includes a consists amount of attacks and can be over a period of time. They are similar as both encounters involve hacking and taking advantage of one(s) information and accounts.

On February 24, 2022, ARcare experienced a data security incident that impacted its computer systems and accounts. ARcare is a company that specializes in discounted medical services and supplies in communities where it is heavily needed. They found out the hacker had access to the companies’ information for a period of 5 weeks. They are investigating and noticed that over 30,000 patients’ information maybe at risk. They are continuing to work on investigating the situation.

Personally, after reading this article I am afraid of my personal information being hacked. Overall, I never give my personal information (Social Security #, address, phone number, etc.) to online websites (at least I try not to), unless it looks secure. For reasons like the current event above, anything can happen and hackers are able to ruin your life just by looking through a computer.

SOURCES:

*Data breach at US healthcare provider ARcare impacts 345,000 individuals*. (2021). The Daily Swig. <https://portswigger.net/daily-swig/data-breach-at-us-healthcare-provider-arcare-impacts-345-000-individuals>

*What is cyberterrorism?* (2020). TechTarget. <https://www.techtarget.com/searchsecurity/definition/cyberterrorism>

Week 5 Journal : Identity Theft

Module 4 : Identity Theft

Identity theft is where someone utilizes the internet or someone else’s personal information to commit fraudulent activities. Identity theft is illegal and can ruin an individual’s financial future. Information like credit cards, social security number, etc. can be utilized to help the thief, thus why we must take action to prevent these situations from happening.

Identity theft penalties vary. If the amount stolen, goods or services are equal to less than $500, then it is only a misdemeanor identity fraud where the guilty person would have to serve 18 months in prison and/or pay a fine of $5,000. If it exceeds the $500 threshold, then the person is guilty of felony identity fraud and can face 15 years in prison and/or a fine up to $15,000.

Someone can prevent themselves from being hacked by identity thieves by encrypting their information or using a password protector. Using difficult or hard passwords to guess are key to keeping important information and accounts locked and safe. Ignoring phishing emails (emails that look suspicious or ask you to click a link) as well are important, as these links may allow malware and viruses to get into your information without you even knowing.

On May 5th 2022, a man living in North Carolina was caught forging deeds and transferring others’ properties to his name. He is charged with grand jury for common law forgery, identity theft and a couple of counts of “…accessing government computers to defraud and preparation to commit housebreaking…”.

This story is very crazy to me, that people will go through such efforts to gain property and information and think they will never get caught. This emphasizes to me even more the importance of keeping things safely secure because you really never know who wants what you may have.

SOURCES:  
<https://maryland-criminallawyer.com/maryland-fraud-lawyer/identity-theft/>

<https://www.usnews.com/news/best-states/north-carolina/articles/2022-05-05/man-indicted-for-forging-deeds-to-steal-n-carolina-property>

Week 6 Journal : Sexual Exploitation

Module 4 : Sexual Exploitation

Sexual exploitation (to my understanding) is where someone or groups of people, may take advantage of others when they are at their lowest and/or may need something. The penalty for sexual exploitation are actually very severe, with the minimum sentence of 15 years in prison and maximum sentence of 30 years in prison.

According to an article published by the Washington Post, they describe that during the Ebola epidemic in Congo, many WHO ( World Health Organization ) members were sexually exploiting women, and promising if they did what they were told they were promised jobs and positions within the agency. Many of the perpetrators were security, drivers, doctors, senior staff, etc. with over 83 allegations.

Personally, it is very disappointing to read this story. WHO is supposed to be a helpful and humanitarian organization, but members are not following the principles. This reflects poorly on the organization especially with all the good things they have done. We must also be careful with who we surround ourselves with as they may only be there to take advantage of one and other.

Week 7 Journal : Social Engineering

Module 5 : Social Engineering

Social engineering is the act of exploiting a person’s weaknesses to gain information about them and in turn benefit in different ways. Different acts of social engineering can include identity theft, phishing and scareware. These crimes can actually happen both in person or online, but more commonly they happen online.

Like many other internet crimes, social engineering can result in a variety of penalties. From just a misdemeanor to jail time. In most cases, the victim can receive financial compensation up to $500,000. But each case varies depending on the circumstances.

One can protect themselves from social engineering in so many different ways! One way is to do two step authentication, meaning attaching a phone number or second email to the account or providing security questions or second passwords. This helps build up another wall for your information. Don’t download suspicious information or links, and install antiware or security software to your devices.

Recently, many cryptocurrency platforms and companies have been receiving phishing attacks. The hackers are trying to receive user’s funds by requesting they transfer/ integrate their crypto-wallets via a third party app. Cryptocurrency platforms like Etherscan and CoinGecko, are trying to combat these attacks by disabling compromised third party integration.

Personally, I believe this story is scary for those involved in cryptocurrency. I believe phishing attacks through email or texts, are less scary because as long as they look suspicious many know not to click those links. But, cryptocurrency is a more professional and a real company that manages financials. Even a small mistake regarding phishing can possibly ruin your entire finances.

<https://www.investopedia.com/terms/s/social-engineering.asp>

<https://www.atrizadeh.com/social-engineering.html>

<https://cointelegraph.com/news/etherscan-coingecko-warn-against-ongoing-metamask-phishing-attacks>