Building an Educational Website

Dedicated to the Study of Violent Crime

Perpetuated Through Social Media

A Master's Thesis Project

Presented to the School of Arts & Sciences

State University of New York

Polytechnic Institute

Utica, NY

In Partial Fulfillment

of the Requirements for

the Master of Science degree

Kristen Maloney

April 2019

SUNY POLYTECHNIC INSTITUTE

DEPARTMENT OF COMMUNICATIONS AND HUMANITIES

CERTIFICATE OF APPROVAL

Approved and recommended for acceptance as a thesis in partial fulfillment of the requirements for the Degree of Master of Science in Information Design and Technology

_____

Date

X

Dr. Ryan Lizardi
First Reader

X

Ana Jofre
Second Reader

ABSTRACT

Computing technology has taken over every aspect of life, from business to socializing, the world is entirely dependent on the Internet. Social engineering, hacking, and phishing attempts have made protecting private information and finances more complex than ever. As new techniques and equipment are created by the day, law enforcement struggles to keep pace. With the rise of social media, online gaming, and crowdfunding, there are more outlets than ever for criminals to attempt to defraud unsuspecting victims. This study serves to examine what makes cybercrime so attractive, the types of attacks and targets, and the role of law enforcement in investigating crimes; with on how social media networks like Facebook or Twitter have allowed crime to cross into real life. Utilizing this information, I have created an educational website for use in public or academic spaces to make cybersecurity information accessible. This flexible platform can be updated in real time as more information becomes available – allowing for new risk and solutions to be added.

Table of Contents

LITERATURE REVIEW

RESEARCH QUESTIONS:

1. What is Cybercrime and how is it relevant to the general public, regardless of their online presence or usage?

2. What data would be necessary in building a comprehensive resource to educate visitors about online threats, ongoing cases, and potential updates to online policies or social platforms?

3. Considering principles of information design and the navigation options presented by a web platform, how can this data be made approachable for visitors of various tech awareness levels while maintaining flexibility for ongoing growth?

History & Tools of Cybercrime

What is considered cybercrime has preceded the mass use of home computers by several years. One of the earliest identified hackers from the 1980s, John Draper aka Cap'n Crunch, made a name for himself as a phone phreaker. Utilizing a toy whistle that gave off a specific tone, he was able to manipulate the AT&T phone system into allowing him to make free long-distance calls. The first conviction came in 1981 when Ian Murphy, aka Captain Zap, was charged with cybercrime for hacking into AT&T to manipulate hourly rates by tampering with internal clocks – a similar tactic utilized by Cap'n Crunch. 1982 brought the first computer virus, made as a prank by 15-year old Elk Cloner that spread infection via floppy disk. (Florida Tech Online, 2018)

The Honey Pot tactic, which is still regularly employed through unsecured wireless connections, attempts to convince victims to connect to a network controlled by a hacker to extract information. First used by Clifford Stoll in 1986, stolen data may be resold to others, or further exploited by the hacker for financial gain. Passwords, internet histories, and other crucial privacy data can be gleaned from this method without victim knowledge. (Florida Tech Online, 2018)

The first malicious internet code – another type of attack that persists to this day, came in 1989 courtesy of Cornell student Robert Morris. A worm is designed to self-replicate, which may assist in the spread of viruses or overwhelming network traffic; Morris' worm, without the aid of a massive online structure we enjoy today, managed to infect 6,000 computers. (Florida Tech Online, 2018)

The first ransomware attack – a method of holding a person's computer, data, or network hostage until the hacker's demands are met, came in 1989 via floppy disk. By distributing software to the 20,000 attendees of the World Organization's AIDS conference, hackers were able to encrypt all data on machines where the software was downloaded and refuse access until a specific amount of money was paid. In this case, the fee was $189 per machine, payable to a PO Box in Panama to mask the identity of the responsible parties. This technique is still widely utilized, famously utilized in the WannaCry attacks on British health systems in 2017 where the attackers demanded $300 in bitcoin (untraceable cryptocurrency) to unlock each machine. (Florida Tech Online, 2018)

The Internet Crime Complaint Center (https://www.ic3.gov/default.aspx) was created in 1999 to deal with the rapidly increasing number and scope of attacks. In the first year of operation, they received 75,000 complaints a year; the following year that number ballooned to over 108,000 complaints. The FBI joined the criminal crackdown in 2002 with the FBI Cyber Division, designed to track "physical crime" that had shifted to the online sphere: identity theft, intellectual property theft, fraud, and cyber terrorism were placed under their jurisdiction. In an effort to create unity across various investigative bodies, the National Cyber Investigative Joint Task Force was created in 2008 to ensure the FBI could share and utilize information made available through various intelligence communities and the Department of Defense. (Florida Tech Online, 2018)

Hackers as early as the 1990s utilized social engineering in order to steal personal information and fraudulently impersonate someone else. Social engineering is a tactic commonly utilized to get information from a well-intentioned or trusting individual without arousing suspicion. Hackers could call credit card companies claiming to be the card holder, giving the phone representative a tragic story about how their card has been misplaced and requesting a replacement be sent to another address. Dumpster diving to research the mark in advance would typically give the hacker enough personal information to convince the credit card company that they truly were the cardholder. The representative, aiming to deliver solid customer service and help the upset person, would likely do as requested without realizing they had compromised the account's security.

This method is still popular and finds success with credit card companies, banks, and cell phone providers. As technology changed and users could see charges in real time on their phone, this tactic sees less success than it used to.

Types of Current Threats

The amount of attacks possible in the cyber realm have only managed to increase. In a study by Brar and Kumar, they warn that,

> "During the last five years, we observed that an increasing number of data, devices, and clouds were forming a perfect security storm of threats. Some of the threat predictions became true which are leading significance of much bigger storm expected in the near future. The dynamicity in the work place, highly mobile work strength, and frequently changing expectations of workers have changed the concept of network boundary. The flood of personal network devices has created an exponential growth of personal data on the Internet." (Brar, 1)

They state that there are three critical pillars of cybersecurity: confidentiality (limiting data to authorized users), integrity (ensures data accuracy), and availability (ensures network access for authorized persons).

These tenants of cybersecurity are regularly under attack in 4 categories proposed by Brar and Kumar: cyber violence, cyber peddler, cyber trespass, and cybersquatting. These categories are further broken down as: world war, terrorism, stalking, revenge, frauds, activism, theft, espionage, pornography, classic squatting, derogatory squatting, and typographical squatting. (Brar, 5) These terms refer to the type of crime being committed, but not the act or design itself. Though several are familiar and have physical

representations in the offline world, issues such as cyber-squatting don't have as strong of an offline counterpart. Cyber-squatting can come in multiple avenues, as listed by the researchers. Classic cybersquatting occurs when an individual intentionally purchases a domain name that was mistakenly not registered first by a famous brand and refuses to vacate without significant financial repayment. For a few minutes, the Google.com domain name left Google's custody and an individual was permitted to purchase the domain. The individual could have held the domain hostage until Google paid the equivalent of a ransom to retrieve it; this case is unlike common situations as Google has the money and connections to force the domain back into their custody. But for less famous brands, this could be a major obstacle. Derogatory cybersquatting is the act of building a website similar to a famous brand or person with the intention of harming their identity or reputation. Typographical cybersquatting is hosting a site with a domain name similar enough to a famous site that you're hoping a typo might lead traffic to the site. In the Google example, purchasing gogle.com might be construed as typographic cybersquatting.

There are 3 principal focuses of cybersecurity, and each can be attacked in unique ways. Confidentiality can be compromised by traffic analysis, eavesdropping, snooping, password attacks, keyloggers, and social engineering. (Brar, 7) The first three of these types of attacks focus predominantly on web traffic – attempting to steal data as it travels in and out of a device. This can also be accomplished via honey pots when users mistakenly connect to an unsecure network, giving hackers full access to their data. Password attacks are more offensive, an effort to forcibly crack a user's password and gain further access; a multitude of programs exist explicitly for this purpose, though the

programmers insist they are not liable if they are used for illicit purposes. Keyloggers are devices that are designed to keep track of every button press on a keyboard for the purpose of password discovery or web history tracking. Keyloggers have been used outside of criminal spaces to spy on loved ones or ensure business information is not leaving a secure space but still maintain mass appeal for criminals. Social engineering is the most cost-effective method with no equipment or software required; a highly recognizable form of online social engineering is phishing. A phishing attempt would come in the form of an email to an unsuspecting user warning of an unknown threat or time critical risk – for example, the email may claim that the user's bank account has been compromised and they must follow the enclosed link to re-secure the account. Clicking the included link would lead to a fake site designed to look like the bank's web portal but sending information directly to hackers. Though many attempts will include incorrect grammar, lack of security, or lack of personalization, these phishing e-mails become more and more sophisticated. Users have been warned by brands and banks to never click links in e-mails concerning security and to reach out to representatives personally or type in the web address in a new window.

Integrity can be compromised by salami attacks, data diddling, cross-site scripting, SQL injection, and session hijacking. (Brar, 7) Salami attacks are minor attacks that are almost unnoticeable, like stealing a few cents from a bank account at a time. Data diddling attacks refer to the illegal editing of data, such as timesheets, grades, or other critical documentation. Cross-site scripting (XSS) is when a hacker includes malicious or harmful information in a website that the victim has been sent to. When they visit the site, malicious code is downloaded and may access personal information stores in the

browser's history. SQL injection attacks are similar to XSS attacks, but they have the ability to go around website authenticators to steal personal information. Session hijacking refer to an attacker's ability to hack into an open session to steal data; this is also referred to a man in the middle attack. When users transmit data to their banking website, it must travel through the network. A hacker could position themselves to intercept that data and gain access to the account itself.

Availability can be compromised by DoS/DDoS attacks, TCP SYN attack, UDP attack, ICMP attack, and HTTP attacks. (Brar, 7) A DoS or DDoS refers to a denial of service attack, one of the most common attacks utilized on the internet. The intention of a DoS is to overload servers with so much traffic that they can no longer operate, shutting down any sites hosted and limiting or eliminating access for a period of time. Attackers utilize bots to create the false traffic rush from their own machine, a server, or unsuspecting machines they have enslaved elsewhere. TCP, UDP, ICMP and HTTP attacks are all efforts to stop traffic to a specific site by overloading or compromising the networking process that allows traffic to pass through.

Who are Hackers?

Though there are countless lone wolf types in the world who aspire for personal wealth, fame, or notoriety, the most damaging cybercrimes are typically the result of organized criminal endeavors with purpose and financing to acquire hacker talent. Leukfeldt examined a series of international groups of criminal organizations and cybercriminals via police investigation in the effort to understand their ranks and how they operate. He identified the following types of criminal group interactions: (I)

Completely through offline social contacts; (II) Offline social contacts as a base and online forums to recruit specialists; (III) Online forums as a base and offline social contacts to recruit local criminals; (IV) Completely through online forums. (Leukfeldt, 2016, 292) When examining the groups, it was quickly ascertained that not every member was a hardened mobster. There were a central few members who would organize a majority of decisions, but hackers were largely disconnected from the internal business and would only perform the duties asked of them. Because of the complex nature of cybercrime, hackers regularly required the assistance of both willing and unknowing partners to gain access or necessary information. The study found that, "In ten investigations, we found evidence of connections between cybercriminals and the legal economy. In three cases, bank employees working in banking call centres and postal workers were involved in the crime script. The bank employees provided core members with information about bank customers and their bank accounts that could be used in social engineering attacks, or they made unauthorized changes in the accounts of customers." (Leukfeldt, 2016, 294)

Organized crime is considered an arrangement with at least 3 consistent members and an established hierarchy with a focus on very specific criminal activities. (Leukfeldt, 2016, 295) Cybercriminals may be utilized for a multitude of cybercrime, expanding their scope well beyond the limited focus of a typical criminal organization. Though they may work in conjunction with a mafia-type group, networks of cybercriminals are not categorized in this study as being a recognized organized criminal entity. The most valid comparison would be hackers operate as independent contractors for the term of the job they're commissioned to perform and owe no loyalty to any singular entity or person.

Selecting a Target

Protection against cybercrime is unlike physical protection methods. Offline, there are common sense social expectations in place to prevent theft or injury: keep doors and windows locked, valuables should be in secure locations, important paperwork in lockboxes, be aware of your surroundings etc. The majority of cybercrime victims don't realize they're being attacked until after the damage is done, which may take months to years to repair. Researchers have examined what type of victim is the typical choice for cybercriminals and what makes them vulnerable. Ilievski writes in his paper, "Through their everyday online activities, cyberspace users are exposed to motivated offenders. In addition to the exposure and proximity of perpetrators, users, with their risky cyberspace activities, and because they do not use adequate protective and preventive measures, could increase the likelihood of becoming a victim." (Ilievski, 2016, 31) This statement summarizes the amount of exposure online that victims don't consider in their usage and the lack of awareness surrounding protection.

Ilievski's research applies Schreck's theory of self-control to discern what may lead to victimization. The six elements of the theory: low future orientation, self-centeredness, low tolerance of frustration and anger, lack of diligence, preference for physical rather than mental activity, and risk taking. These elements work in conjunction with one another to create the vulnerabilities that may make someone attractive to target or likely not to suspect ill intent. A low sense of future orientation insinuates no thought to the long-term consequences of actions; self-centeredness leaves the potential victim to only see themselves and not consider the motivations of those around them. Low

tolerance for frustration allows someone to yield to a potentially bothersome attack if it ends the action, and lack of diligence refers to individuals' lack of consideration for protective or proactive efforts. Those who think about physical actions more than mental do not consider cyber risks, which also plays into the personality of risk takers who do not analyze the potential fallout of their actions.

Ilievski also examines victimization from the approach of the lifestyle/routine activity theory (LRAT) created by Cohen and Felson. They argue that, "crime as a non-accidental phenomenon in society is dependent on three components: a motivated offender, a suitable target and lack of capable guardianship." (Ilievski, 2016, 35) The theory of LRAT when applied to cybercrime focuses most intensely on the first component: a motivated offender. The scope of the Internet being so wide, the amount of potential victims and their lack of protection is enormous, leaving malicious actors boundless opportunity. In citing another study concerning online activity and victimization, Ilievski includes the deductions of Van Wilsem who studied the factors which affect the occurrence of any digital threats (by e-mail or online chat) and found that the use of webcams, social networking and intensive online shopping are factors which increase the risk of victimization. In another study Van Wilsem (2013) concluded that the above lifestyle/routine activities are significantly associated with harassment and "hacker" attacks victimization together. (Ilievski, 2016, 36-37) The research of both authors demonstrates that those who expose themselves more openly and share details of their lives on social media are more likely to become targets of hackers and potential harassment. This theory is proven in practice by the amount of celebrities, political

representatives, and other recognizable personas that regularly must face regular harassment and compromising attacks.

The common trends in victimization is further justified by Van de Weijer and Leukfeldt in their research on the subject; their deductions nearly align with the six personality traits identified by Ilievski with some additional details discovered through qualitative research. In comparing the data, it was discovered that:

> "Results showed that lower scores on conscientiousness and emotional stability and higher scores on openness to experience were significantly related to victimization risk of cybercrime…Against our expectation, however, only conscientiousness was shown to be related to cybercrime victimization in the current study, while no significant relationship was found with agreeableness. In addition, also lower scores on emotional stability and higher scores on openness to experience were shown to be associated with cybercrime victimization." (Van de Weijer, 411)

In short, persons who were more open and trusting, wishing to make others happy without conflict, were found to be the most vulnerable parties. These studies justify the practice of social engineering and why it continues to be so successful after decades of use.

Despite all protections, awareness, and deterrents, it is still possible to be a victim of cybercrime. The research and observations of the authors noted trends that help demonstrate how cybercrime can continue to be so prevalent, especially given a pool with millions of potential victims around the world. Protective measures, awareness, and a

healthy amount of suspicion are the recommendation for online safety from researchers and security professionals alike.

Crime as a Business

Hackers are typically not the masterminds of criminal organizations or dedicated loyal soldiers to a particular crime family. The fruit of their labor is typically offered up on the black market to the highest bidder, creating a unique economy in the acquisition and resale of compromised personal information or access credentials. Yet in recent years there has been a shift in cybercrime to a less isolated operation to something akin to "crime as a business". By stealing information in bulk and selling the most vulnerable or important data to the highest bidder, hackers can turn enormous profits instantly. Those returns increase exponentially when a dedicated team of hackers sets to work acquiring a massive cache of intel. The issues presented in building a cybercrime-driven economy are studied by researchers Kesari, Hoofnagle, and McCoy. Addressing some of the obstacles, "In both the illegal goods and infringing goods contexts, each critical function to monetizing the crime relies on third party intermediaries. Sellers and marketplaces need domain names, hosting services, access to payment systems, banking services, access to postal or shipping networks, and so on. Many of these intermediaries are probably unaware of misconduct." (Kesari, 1100) This issue raises a series of legal questions for the unwitting parties that may be involved in the exchange of stolen material as well as the jurisdiction where the crime may originate.

Successful business ventures require a variety of markets for the enterprising cybercriminal, which requires law enforcement to be prepared to react. Botnets and third-

party sellers of illegal goods are some of the most powerful tools in a hacker's arsenal – though they are not immune from law enforcement's efforts. The study explains that, "Botnets are networks of infected computers (the "bots") that are used to conduct illegal operations. In particular, botnets can be used to forward communications (i.e. spam emails, viruses, etc.) to other computers and grow the network, and to execute Distributed Denial of Service (DDoS) attacks that can disrupt all internet use." (Kesari, 1102) Essentially an army of machines performing the same function at the command of a single hacker can be deployed to targets anywhere in the world without any knowledge of the computers' legal owner. Kesari explains how despite the various location and amount of machines, companies like Microsoft have created tools to combat botnets by seizing control of the domain.

Third parties have been a necessary part of black market or illegal product movement since the dawn of crime. Hoping to keep their identity hidden, hackers rely on these intermediaries to broker deals that may turn their criminal efforts into profit. Jurisdictional limits typically prevent the physical arrest of known illegal dealers around the world, though steps can be taken to seize and shut down any domain or online hub they may have utilized to conduct exchanges.

Some of the most critical entities in battling cybercrime are intellectual property owners; a brand is only worth as much as can be protected. Companies and persons may face risk to their reputation and business when allowing infringing claims to dilute their property. Laws surrounding copyright and trademark share international recognition (https://definitions.uslegal.com/i/international-copyright/) in many ways, avoiding the issue of

limited jurisdiction when attempting to shut down counterfeits or other illegal actions involving protected properties.

Researchers Konradt, Schilling, and Werners took an in-depth look at the financial impact of these criminal enterprises, specifically focusing on the common tactic of phishing, which requires more than a single hacker to draw a profit:

> "There are four main actors involved in phishing attacks: a coder, a group of fraudsters, a broker, and a buyer. In the example of obtaining bank account credentials, the coder is responsible for creating a spam mail and implementing a malicious copy of a bank website. This website transfers bank credentials or other sensitive information entered by the victim directly to the perpetrators. In this case, the coder is an independent actor and, therefore, sells the malicious software to the group of fraudsters. They use this software to carry out the actual attack and possibly reuse the same software for following attacks on other computer systems and networks. After the fraudsters have obtained the targeted information, they sell the stolen data on a black market to potential buyers through brokers. A broker simply acts as an intermediary between the two parties." (Konradt, 2015, 40)

In the example provided, only one party interacts with the victims, and the buyer has no record of specifically how and from whom the data they're purchasing was acquired. These levels of secrecy are what allow cybercrime to spread, evolve, and endure.

Given the enormous amount of information online and the constant rate of change, the assumption that may be drawn is that cybercrime isn't as severe or wide-

reaching as some would make it seem. Because of these misconceptions, law enforcement is years behind in technology, funding, and manpower to meet the threat head on. In an article written by Nir Khestri, he observes, "Digital criminals are also more difficult to catch and prosecute than conventional ones. In fact, collection and retention of evidence has been a critical challenge facing law enforcement agencies. Estimates suggest that the U.S. Department of Justice declines to prosecute up to 78% of cases mainly because of a lack of evidence. Cybercrimes' newness has also presented challenges to the court system. For small cybercrime cases, it is difficult to find an attorney. Experts also say that explaining cybercrimes to judges is difficult." (Khestri, 143) When considering the enormous cost that these crimes place on the economy, Khestri summarizes his article in closing that, "Cybercrimes are costing businesses, especially banks and credit-card companies, and consumers billions of dollars every year. For instance, in 2006, the cost of identity theft, a significant proportion of which is facilitated by the Internet, was estimated at over $50 billion to U.S. businesses plus $5 billion in out-of-pocket expenses." (Khestri, 144) These billions of dollars increase every year and open consumers to enormous financial and personal risk.

Efforts are being taken to understand the nature of cybercrime and what makes it so financially successful yet legally difficult to track and prosecute unlike similar physical crimes. Khestri's article gets to the heart of the issue: an untrained and unprepared legal and law enforcement system provided the opportunity for these crimes to grow unchecked. Technology is invented daily in conjunction with cybercrime task forces around the world and international policies are being written, but the pace at which

the laws are being signed or investigation budgets increased is not nearly fast enough to deter the billions of dollars in easy targets for professional hacking enterprises.

Economic Inspiration

Though cybercrime can originate anywhere in the world and impact someone thousands of miles away in another country, researchers questioned whether the country of attack origin may play a role in the multitude and type of attacks. Aleksandar Ilievski and Igor Bernik examined the social-economic factors that might impact cybercrime. Citing two additional studies, the researchers found that, "There is a correlation between the cyber attacker's computer expertise and the degree to which a given attack is successful. Escalating levels of unemployment among people with a significant knowledge of computing and informatics might turn out to be among the important cybercrime factors. For instance, the Nigerian group "yahooyahoo boys" which is one of the best known cyber fraud groups in the world, is made up of uneducated young people with exceptional computing skills and expertise who live only on the profit made by frauds (Ehimen and Bola, 2010; Ojedokun and Eraye, 2012). In a very similar study Warner (2011) found that the members of the group "Sahawa boys" engage in cybercrime as a means to survive during periods of unemployment."(Ilievski/Bernik, 2016, 9) The stark comparison of these two groups is clear: one relies entirely on fraudulent income to survive, while the other only turns to crime as a necessity to maintain their income while unemployed.

The theory the researchers were endeavoring to prove, known as Strain theory, was that lack of gainful employment would typically lead people to lives of physical

crime, and the same would apply online. In summarizing Strain theory, Timothy Brezina found that stress and negative emotions (anger, depression, desperation etc) were a driving force that inspired people to justify criminal action. (Brezina, 2017, 1) After World War II, the economy of most countries struggled to recover, leading to poverty and mass unemployment. This lack of direction led people to pursue knowledge wherever possible, despite the inability to find a job. Applying these skills to illegal enterprises was enough for desperate people to survive; discovering the ability for enormous wealth through crime maintained the criminal economy. When applying the Strain theory, researchers could see that a culture lacking in economic strength and strong legal protection allows for the ability of delinquent subculture and criminal enterprise to thrive. Where there is a lack of legitimate opportunity, people will find themselves forced to earn money through illegitimate means in the name of survival. (Ilievski/Bernik, 2016, 14-15) By this regard, poorer nations are more likely to see a rise in criminals, both offline and on; cybercrime is more attractive due to the lack of physical risk and legal failings that prevent most hackers from being caught.

When a Crime is not a Crime

Before Facebook took hold of the social media world, MySpace was the home of teenagers eager to form their online identity and connect with friends, bands, and the odd potential romantic partner. On October 17, 2006, 13-year old Megan Meier took her own life following a series of exchanges on MySpace with 16-year old Josh Evans, who had expressed romantic interest only to brutally turn to bullying. The young girl, previously diagnosed as suicidal in addition to attention-deficit disorder, depression, and lacking

self-esteem, was already a habitual victim of bullying in school. When investigators started unraveling the details leading to Megan's tragic death, they came upon a shocking revelation: Josh Evans was not real. He was a MySpace account specifically created to hurt Megan by 47-year old Lori Drew, mother of schoolyard bully Sarah Drew. The Drews and other schoolmates utilized the account to torment Megan Meier, telling her in the last fateful exchange that, "the world would be better without you." Megan was found dead an hour later. (Zetter, 2008)

The Megan Meier suicide case was a hotbed of discussion about online conduct, legal limitations, and ethical standards of each. During the trial, both Drews were not remorseful of their actions, though both testified they had knowledge of Megan's mental health history and potential for suicide. Neither took responsibility for their actions. There was a significant amount of discussion about the terms and conditions of MySpace itself, which barred profiles for users under 14 (both Megan and Sarah were underage). Though MySpace had provided the platform, they could not be found legally liable for the conduct of their users or expected to police the thousands of accounts added every day that only required an email to set up. Lauren Collins writes in The New Yorker online:

> "Lori Drew called the police. According to the police report, she "wished to inform law enforcement about a neighborhood dispute." This was the report in which Lori admitted to being actively involved in—rather than, as she now contends, vaguely aware of—the Josh Evans hoax. Lori told the police that she "felt this incident contributed to Megan's suicide, but she did not feel 'as guilty'

because at the funeral she found out that 'Megan had tried to commit suicide before.' " (Megan had never tried to commit suicide.) " (Collins, 2008, 57)

Lori Drew was indicted and convicted for violating the Computer Fraud and Abuse Act in 2008, a decision that was later vacated. The opinion of the court was, however despicable the actions of Lori Drew, she had not violated the law as it was written. The government decided not to appeal and the case was put to rest. (DLMP, 2008) The lack of justice for the Meier family and the shock of the story led towns around the country to create laws criminalizing cyberbullying and/or cyber harassment. Congresswoman Linda Sanchez sponsored an amendment to title 18 of the US Code in 2008 to protect future victims referred to as the "Megan Meier Cyberbullying Prevention Act"; it never made it past committee review. (Cox, 2009, 1)

Digital Crimes with Offline Consequences

On December 27th, 2017 in Wichita, Kansas an online game of Call of Duty resulted in an argument between friends Casey Viner and Shane Gaskill over a $1.50 bet. The argument escalated when one of the gamers asked another party, Tyler Barriss, to "SWAT" the accused player to get revenge; SWAT-ing is a practice where an individual calls in a fake hostage situation at a specific location (typically the home of someone they wish to terrorize) to trigger a SWAT team deployment. These types of attacks waste valuable time and police resources, though prosecution has been difficult as the calls are typically across state lines and instigated by minors. This case ended in the accidental shooting by police of Andrew Finch, a 28-year old man living at the past address of one of the gamers. This was the first documented incident of injury leading to death related to

the online pranking practice gone wrong, and the parties involved faced legal action. Tyler Barris, 25, faced over 60 federal charges, pleading guilty to 51 concerning fake bomb threats, financial fraud, and involuntary manslaughter. Prosecutors are asking for a 20-year sentence with an additional five years' supervised release and a $10,000 payment for fees and restitution to the Finch family. State charges are still pending. Gaskill and Viner also face federal charges for wire fraud, conspiracy to obstruct justice, and conspiracy to make false statements; they currently face up to 60 years in prison. Shane Gaskill went to far as to attempt to convince Barriss to make another SWAT-ing attempt after causing the wrongful death of Andrew Finch, resulting in additional charges.

The Wichita Eagle reported that Barriss had a history of calling in fake bomb scares and SWAT attempts to schools, malls, television stations, personal residences and government buildings (Leiker, 2018, 1-4). Despite years of deviant behavior, authorities had been unable to hold Barris accountable for his crimes due to outstanding cases in numerous states and the charges never reaching the level of federal attention. This case demonstrates how easy it is for criminals to slip between the lines online and the legal confusion surrounding jurisdiction and the appropriate charges to be brought against activities that the law had not predicted. Online harassment is a common complaint, especially in the online gaming space. Responding officers have no way of distinguishing a prank from a serious threat and are charged to react appropriately, arriving armed and ready for assault. In Finch's case, he was curious about the flashing lights from officers outside his home and opened the front door to investigate. Officers believed him to be the hostile party they were informed of and opened fire. In ensuing investigations, Officer

Justin Rapp, who fired the killing shot, was cleared of any wrongdoing and defended himself by stating he was responding to the situation he believed to be at hand.

Legal Failures & Pending Legislation

The legality of cybercrime prosecution is lacking at best. Due to the complex nature of the crime, complications over jurisdiction, international policies, and constantly evolving techniques designed to work around current legal restrictions, the law is still catching up to the abilities of hackers around the world. The knowledgeable and professional security professional is typically the best defense an organization has against these types of attacks, but the ability to protect oneself physically, digitally, and legally, have limitations. Most personal victims do not feel the need to hire a professional to implement digital protections, nor do they have the budget to maintain it. Corporations typically employ professionals to investigate, attempt to hack into, and then fortify their online structure; ethical hackers are at the forefront of online protection and may offer their services free of charge or advance contract. These attempts to discover a compromised system can skirt legal laws surrounding consent, an issue Romanian courts felt obligated to resolve. In his paper summarizing the concept of victims consenting to their own violation through ethical hacking, Dobrinoiu writes, "Things are more clear and simple when the person authorizing the hacking is the real owner of the affected value and has the legal ability to dispose of his own values (ex. computer system, computer data). The scenario becomes more complicated when the values protected by the law belongs to the state – through the patrimony of a public institution/authority. According to many authors, if the values targeted by the perpetrator's actions are bound to so-called

collective rights (such as national security, state authority, public trust, public safety, family etc.), these values cannot be protected by the justifiable clause (legal defence) of consent." (Dobrinoiu, 175) Though the intention of ethical hacking is sound, the defense that it is permissible to use these skills to hate federal or state targets does not hold. Consent can be given for direct ownership of the property being hacked, both from a personal or business scale; a government management official cannot grand the same consent from their position. Decisions about allowing a government database to be intentionally compromised could create risks to national security or other internal failures that could cripple the system for days.

The legality of ethical hacking and its role in information security is a minor concern compared to the legal hurdles facing cybercrime prosecution. Vulnerability assessments, prevention methods, and the ethics involved all pave way to the harder question: what should constitute a crime? Should all physical crime with a digital equivalent face the same or similar punishment? The answer to this would typically be agreement in cases of theft, fraud, or malicious action resulting in injury. But when considering physical death versus digital death, are they worth the same sentence? Researcher Litska Strikwerda asked these questions in her analysis on virtual crime regulation from philosophical, legal, and economic perspectives. Killing someone in the physical world is tangible and clearly has severe consequences; how should an online player be punished for repeatedly killing another player to disrupt their enjoyment of the gaming experience - known casually as "griefing". In the analysis, the argument is that imposing the same laws that apply in the physical world would restrict and unjustly punish virtual actors as they are unable to create the same permanence as the crimes'

physical counterpart. These punishments would infringe on individuals' rights, freedoms, and ability for self-expression. Adding dozens of cases to the legal system for virtual crimes that might be perceived as frivolous would impose an undue workload on the judiciary as well as inappropriately burden prosecutors attempting to settle physical criminal cases.

Child pornography including actual children in a physical space that engaged in sexual acts is illegal in film, print, or production, as well as sharing with any parties online or off. To work around these legal restrictions, predators have begun to create "virtual" child pornography using digital children who never existed or manipulating images of actual children into actions they've never performed. (Strikwerda, 34) According to the letter of the law, these virtual creations do not represent an event that occurred with physical people in a physical space and were not initially subject to the same laws that govern the offline crime. The inability for the law to not only anticipate these loopholes but correct them in real time leads to the rapid propagation of criminal enterprise in virtual spaces. The Convention on Cybercrime, introduced in 2004 yet not effective in the US until 2007, ruled that virtual child pornography would be considered equivalent to its physical counterpart; the United States was unable to fully implement this ruling as it ran counterintuitive to the First Amendment protections of the Constitution, forcing a Congressional action that specifically redefined what would be considered child pornography.

One of the issues that gives rise to cybercrime is the ability to connect with like-minded persons and hide behind the assumption of anonymity; hate groups, child

pornographers, hackers, and malicious gamers have all found protection because of these attractions to the virtual space. Strikwerda discusses some of the most pressing details when trying to prosecute and prevent the spread of malicious online behavior, but the obstacle of distance is the first to come to mind. Geographic obstacles can make it difficult, if not impossible, to take persons of interest into custody; international treaties and extradition agreements are critical in successful prosecution of virtual criminals. The ease provided by the digital landscape allows for millions of unsuspecting targets around the world for the motivated hacker – which could create a multitude of overlapping extradition claims when they are discovered. These international negotiations could play out for years as countries argue over jurisdiction, amount and type of criminal charges being considered, and the location of the accused. (Strikwerda, 54)

The ability to communicate openly, efficiently, and immediately between law enforcement agencies around the world has become one of the most critical aspects of battling cybercrime. In his article on extradition cases and existing law-enforcement agreements, Gregor Urbas gives specific examples of complex international criminal investigations that yielded arrests in several nations around the world. These agreements between jurisdictions have been the result of years of policy making and negation and continue to improve over time. “In the most sophisticated of such co-operative arrangements, law enforcement agencies in several countries are able to share operational information and co-ordinate critical actions in real time so that search warrant executions and arrests occur simultaneously in different locations across the globe. Clearly, this is important in ensuring that all members of globally dispersed groups can be apprehended before they have an opportunity to flee or to destroy evidence. Significant internationally

coordinated enforcement actions have been reported against international child exploitation rings and global copyright piracy groups." (Urbas, 2012, 9) The online world is constantly in rapid motion, giving ample time for crimes to be committed and disappear into the ether again without a trace; law enforcement needs to be able to react faster than the criminals can attempt to disappear. Urbas includes cases involving child pornography, stalking, intellectual property theft, and counterfeit game sales that could not have been closed without the cooperation of agencies around the world.

Extradition of criminals is only part of the legal issue to be considered; how do countries respond when the accused is part of a state-sanctioned hacking initiative? In recent years, the occurrence of nations utilizing discreet hacking operations to acquire knowledge about their adversaries has seen a dramatic rise. The ability for digital spies to sneak in and out without physically risking capture or torture is highly attractive to state sponsors; hackers desire to work outside of typically government hierarchy to maintain their individuality and freedom serve this purpose well. Researchers Eric Blinderman and Myra Din sought the answers to these questions by examining some prominent cases of state-sponsored attacks on corporate, financial, and political targets within the United States. The authors define an attack by a state sovereign as, "as any digital activity which runs afoul of US domestic criminal statutes…sovereign attribution to cybercrime should attach when any individual, arm, or agency of a sovereign acts, or acting at the direction of a sovereign, is directly responsible, aids or abets those responsible, conspires with those responsible, or otherwise facilitates the perpetration of such cybercriminal activity." (Blinderman, 2017, 894) The study refers to incidents involving Chinese, Russian, and Iranian attacks on US targets with significant evidence and identified culprits; though the

accused were indicted, the sovereign nations that sponsored their actions would not acknowledge the crimes or allow for the extradition of their actors.

Of the cases examined, the most controversial at present is the discussed Russian attempt to influence the United Stated elections in 2016. To summarize the case: "In January 2017, the U.S. Director of National Intelligence released a comprehensive report entitled Assessing Russian Activities and Intentions in Recent US Elections. The report observed that Russian cyber activities went far beyond the mere theft of email and information from the DNC. It described how Russian President Vladimir Putin and the Russian government employed a unique strategy that blended covert intelligence operations with overt efforts by state-funded media, third party intermediaries, and paid social media users (trolls) to gain access to and information from specific targets of both major political parties, which was then relayed to select media sources." (Blinderman, 902-3) The operation began in 2015 and worked tirelessly for months, even until the election itself to compromise Democratic party leaders. During the summer of 2006, using spear phishing techniques (a phishing attempt directed at a specific person), they were able to acquire access to email accounts belonging to Billy Rinehart and John Podesta, the Clinton regional field director and campaign manager respectively. The repercussions of this attack would be felt for the months leading up to the election and are credited at potentially sowing enough doubt to cost Clinton the win. At the time of the researchers' work, no Russian agents had been identified publicly or indicted for their actions despite clear violation of US domestic policy and legal statute.

From January 2017 when the attack was publicly confirmed and Fall 2018, over a dozen Russian actors have been indicted for cybercrimes related to hostile actions against the United States. At the time of this review, Russian President Vladimir Putin continues to deny any wrongdoing from his cabinet, the Russian intelligence service (the GRU), or any independent actors that may have been working for Russian interests. The indicted attackers have not been made available to US authorities for questioning or extradition, nor is it believed they will be.

Conclusion

There will never be a foolproof strategy for combating every type of cyberattack; understanding the motive and vulnerabilities present in online behavior is a start to prevent becoming a victim. As crime evolves, so too must legal policy and law enforcement's ability to investigate, identify, and apprehend cybercriminals. International cooperation is a vital part of the endeavor to protect online activity though research has demonstrated that not every nation has cohesion in mind; state sponsored cyberattacks are largely successful and go without punishment to avoid international conflict. These issues will continue to evolve and challenge traditional ideas of legality, ethics, and philosophy. What constitutes a cybercrime? By what means should it be investigated? How much privacy are we willing to surrender in the name of protection? The current reach of US law can only partially answer those questions.

METHODOLOGY

Introduction

The lack of awareness surrounding criminality online, specifically cases that result in death or serious injury, continues to grow. As the news cycle spins faster in the digital age, it can be difficult to see the dangers associated with social media use. Knowledge is the first step to protecting oneself, both from violent actors and the temptation of negative actions on one's own part. The flexibility and accessibility of a website is a logical solution to this concern; offering a backdrop of cybercrime information as well as victimization preferences, an educational resource utilized by all ages can be crafted.

Social media is a broad topic on its own, so I plan to hone on a series of specific criminal cases that demonstrate the reach and risk of social media use. Unlike typical password phishing attempts or identify fraud, social media's anonymous connections have allowed for criminal actions to reach beyond the keyboard. By detailing these specific cases, as well as utilizing available behavior theory, the website will serve not only as an information source about factual events but also exploring what may have triggered these tragedies. Facebook Live has enabled murders, suicides, and other gruesome acts to be broadcast in real time for the world to see – typically hours before moderators can intervene to stop the content from continuing to post. These case studies will seek to answer how social media has empowered and enabled criminals' brutality, as well as posit the question of how we can counteract these changes in criminality.

Websites operate as platforms that can be regularly added to via content pages, resource additions, or regular blog posts. This range of information types I feel is the most effective way to reach a broad audience who share these concerns or may possess a curiosity about these violent events. In the process of researching material for this study, additional crimes may occur, which can be incorporated into the final product instantly. The unfortunate commonality of these crimes forces me to consider a platform that can easily grow with the necessary discussions that will result from these tragedies.

Planning the Design

Website design comes down to the critical step of simplistic understanding. Navigation should easy and smooth for visitors, no matter their amount of web literacy. A navigation bar at the top is typical for most current pages and allows for an easy separation of topics for quick reference. Those subjects can be further divided by posts relating to specific topic, historical reference, or case study. Keeping the navigation straightforward will serve the most efficient use of space, preferably using bold or bright text to highlight the section titles.

When discussing crime, one typically thinks of bars, black and white, or gray; these tones convey a level of seriousness and force the viewer to accept the words as fact. I included shades of blue in my design to break up the monotony of the darker tones. Blue is a relaxing color that makes viewers feel relaxed and soothes anxiety; because of the delicate nature of the website, I want viewers to feel comfortable engaging with the material. It may be difficult to accept at times, and the calming presence in the design

will assist with that. For visuals I chose standard stock imagery that doesn't distract from the information provided, though some posts may require specific examples, screenshots, or images to correlate with the included information. Concerning the types of cybercrime historically reported, visual examples will be provided to give further texture to the explanation. For example: explaining the concept of "trolling" to set the foundation of negative social behaviors will require a screenshot of such interactions to give the unaware a clear understanding of the topic.

Gathering Resources

The literature review data lays out the groundwork for cybercrime history and some details concerning current risks. The case studies included are an example of the type of material that will expanded upon for further study. These cases are extremely current and there is a significant lack of academic material studying their causality and the repercussions on digital social activity. News reports and preliminary expert analysis will provide insights into these events though they will lack the scholarly credit seen in the historical material.

Utilizing my research on behavior in gaming and social spaces, I can correlate the type of personalities that may lean toward specific types of crimes or online activities. Bad behavior online is not a small issue; many of those bad actors hide behind a screen and never enact physical violence. The anomalies in these groups of online attackers – radicalized individuals or other emotionally stunted persons, are the focus of my study. Utilizing the factual report of cases as they occurred and the difficulties law enforcement

may or may not have encountered in their prosecution, the research can further demonstrate why containing these issues is so difficult.

PROJECT: WEBSITE DESIGN

Choosing a Platform

Wix is a website platform that allows the user to just insert the content as they go with a multitude of display options for unique and interesting content. The design process is easily navigated and visual changes can be seen in real time. The amount of options for visual display easily surpasses its competitor – Wordpress, and the accessibility makes the site easier to manage from an administrator level. Building a platform should always include the conception of being future proof, which means choosing a system that would be easily understood by later additions to the team. The majority of my project relies heavily on the use of textual design that must be easy to read, engaging to the viewer, and comprehensive. The ability to build pages with varying text-based visuals allows the content to be broken up organically on the page without forcing the viewer to navigate complex formatting options.

Text & Visual Composition

For my text choice, I utilized a very clean font entitled, "Agency"; Wix describes it as "smart and professional with a distinct sense of confidence". The information included on the website is serious and should not be taken lightly – I chose a professional font style to emphasize that point. The Internet is largely considered to be a fun place of limitless creativity; criminal actions are not fanciful and must be treated with respect. Legal matters are also typically represented in formal fonts such as Times New Roman, which Agency closely resembles. By utilizing a font that is visibly directing the viewer to

understand the weight of the content they're reading, I could communicate the urgency and importance of the date without harping on the point verbally.

Textual placement I wanted to keep easy to read and separated by differing data dependent on section/theme. In Figure 1, the navigation bar at the top of the site clearly allows for easy access to additional portions of the site. The sections are given simplistic names so as not to confuse the viewer and are not overwhelming in amount. This landing area is the first point of contact for visitors and where they should feel the most welcome. The background image of the library hammers out the idea that this site is a resource, full of data and information that may enrich the mind. The top navigation option allows the ability to visit various parts of the site without fighting with the back option or trying to sort through cumbersome drop down menus – the presentation is clean and contemporary to match with the aesthetic of approachable educational material.

Figures 2 through 6 are screencaps of examples of the type of content in each section the viewer would expect to see; Cybercrime vs. IRL, History, Types of Attacks, High Profile Cases, and Resources round out the initial offerings. The design of each page is contingent on the type and quantity of material that must be addressed. Figure 2, depicting the Cybercrime vs. IRL section, is a pale blue with a wall of text. That information, courtesy of the literature review research, gives the audience a grounding point to understand what allows cybercrime to continue to be perpetuated despite ongoing legislative battles. Much like a legal brief, I wanted the context to be immediately obvious and focused entirely on the text to convey the point without visual distraction.

Figures 3 and 4 are demonstrating the History and Types of Attacks pages, both of which exist to summarize large bodies of information into a concise and easy to follow series of steps for the viewer. The timeline moves from oldest instance to most recent as the viewer scrolls down, each pivotal moment a separate "section" of the page with a shift in color. This design concept was intentional to prevent the text from becoming a wall of characters that bore the viewer and encourage shifting away. Figure 4 detailing the attacks takes a more minute approach, encapsulating each technique in a smaller square like grid for quick reference. Due to the potential complexity of attack methods, I endeavored to keep this information accessible and concise, ideal for visitors with various levels of computer information awareness.

Figure 5 demonstrates the High-Profile cases section – something with a design approach unique to the rest of the page. Utilizing the built-in blog design provided by Wix, I opted to include each case as an individual blog post. This allows for several cases to be posted in simple succession and viewers can glance through the cases that interest them. The cases are not required to be read in any particular order and do not reference one another, there is no need for additional navigation or cumbersome subcategories. As the resource grows over time, it may become necessary to divide cases depending on the type of crime, target, or eventual outcome. The blog formats include the short details of the case and current legal standing as well as a single image to give the reader a visual reference of the accused.

Alternating the visuals styles in subtle ways allows visitors to see something fresh on every page without creating a visually jarring experience. The color palette of grays,

blacks and blues is consistent throughout the site to encompass that confidence I wished to portray while discussing law and order, get demonstrating that not every issue is as clear cut as it may seem. The lack of visuals ensures that the information isn't lost in a distracting wall of images, though the relevant material can be added as the content on the site increases.

Building Content

For the site's content, I utilized the research portions of my literature review as a basis in the prototype. I had already established information about what constitutes cybercrime, the types and history thereof, and challenges being posted by current legal restrictions. By highlighting specific cases with an emphasis on social media, my concept would be to grow; the multitude of risks associated with constantly connected digital personas, a wealth of personal data being surrounded to powerful social media companies, and the end of privacy could be addressed. An early prototype for this resource focused entirely on social media criminal cases, but the lack of academic or professional research on the subject made that unreasonable at this time.

In the light of recent criminal acts involving social applications such as Uber, 4chan/8chan, Facebook, and Twitter, it is evident there will be a consistently growing body of information related to cybercrime and how it connects to actions in the offline world. I brought a handful of that data forward as a foundation for this resource but chose a platform that is flexible and can be easily added to over time. Things that may seem established now like history and types of attacks will evolve – one of the ongoing challenges law enforcement faces in confronting and controlling criminals. The purpose

and design of attacks has also evolved beyond the days of young hackers breaking into secure sites for bragging rights. Hackers are being utilized for identity theft, financial crime, political purpose, and countless additional criminal actions hidden beyond a keyboard. The concept of cybercrime is evolving, and hackers are not the only persons committing illegal actions using technology – as my research demonstrates in the cases provided. There are a multitude of cases concerning white nationalist recruitment, political dissidents, domestic issues that turn violent, or other impulses that make normal people conspire to abuse technology to hurt others – information that can readily be added to this platform and shared around the world for quick access and self-education.

Conclusion

Cybercrime will never be entirely eradicated – but education that arms potential victims with defense tactics and how to respond are necessary to lessen the harm. Online access did not come with instructions or a code of conduct, which leaves vulnerabilities for users who don't consider the risks involved. Social media has opened more holes in privacy than predicted at its creation. This web resource exists as a platform that can be continually added to because of the flexibility of the platform. As information continues to change, the topics, sections, and design will as well. To spread the use of the site, grassroots methods will need to be employed started at the most accessible level – schools. Teaching young users valuable online safety lessons ensures they are responsible users over time and are poised to share their knowledge with peers and elders.

Preliminary visits to the site have shown approval of the steam-lined design, making it accessible to the most casual online user. Keeping complex topics like hacking

techniques and legalese simple keeps the material understandable for the beginning learner. The ability to add current events demonstrated the ongoing risk poised by cybercrime and gives context to the ongoing threats faced by users. The color scheme maintains the calm yet professional demeanor of the topic without distraction or overbeating visuals that tire the eye. The ability to grow the platform with additional material will ensure that this platform benefits a multitude of users on a consistent basis long beyond its creation. Regular updates could make this an invaluable tool to young and old online users as well as create a space for academics to learn the basics of cybercrime to expand their research. As material is limited on the topic at this time, so too will the platform reflect that shortfall.

The topic of my research being compiled and displayed on a website is the more appropriate use of the material. The initial concept of the internet was to allow people around the world to connect and exchange information; that concept did not consider the potential for criminal exchange. This platform sets a foundation for collecting critical educational resources in one place to prevent further victimization while raising awareness for interested parties to expand on the work. As the early pioneers of the Internet desires to connect to other people to grow their fledgling network, so too can this platform be utilized to connect interested parties and build resources through collaboration. To be a successful educational resource, it must be utilized, and the best place to start is where academic learning begins – school. As crime evolves, the platform will have consistent content to add to its curriculum.

Website Link: https://epidemiczero.wixsite.com/website

REFERENCES

Blinderman, E., & Din, M. (2017). Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime. *Vanderbilt Journal of Transnational Law*, *50*(4), 889–931. Retrieved from http://sunypoly.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=127161986&site=eds-live

Brandom, R. (2017, Mar 6) UK hospitals hit with massive ransomware attack. *The Verge.* Retrieved from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

Brar, H. S., & Kumar, G. (n.d.). https://doi-org.sunypoly.idm.oclc.org/10.1155/2018/1798659

Brezina, T. (2017). Feb. General Strain Theory. Retrieved from http://oxfordre.com/criminology/abstract/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-249

Collins, L. (2008, Jan 21). Friend Game: Behind the online hoax that led to a girl's suicide. *The New Yorker*. Retrieved from https://www.newyorker.com/magazine/2008/01/21/friend-game

Cox, J. (2009) May 8. Internet harassment and the First Amendment: is cyberbullying a felony? *Network World from IDG.* Retrieved from https://www.networkworld.com/article/2235642/internet-harrassment-and-the-first-amendment--is-cyberbullying-a-felony-.html

Digital Media Law Project, DMLP Staff. (2008) September 6. United States v. Drew. Retrieved from http://www.dmlp.org/threats/united-states-v-drew

Dobrinoiu, M. (2017). The Consent of the Victim as Legal Defence in Cybercrime cases. *Challenges of the Knowledge Society, Vol 7, Iss -, Pp 174-176 (2017)*, 174. Retrieved from http://sunypoly.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.54be5e9b71f44e99a2837467c7ae0765&site=eds-live

Florida Tech Online. A Brief History of Cyber Crime. (n.d.) Retrieved from https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

Ilievski, A. (2016). An Explanation of the Cybercrime Victimization: Self-Control and Lifestyle/Routine Activity Theory. *Innovative Issues and Approaches in Social Sciences, Vol 9, Iss 1, Pp 30-47 (2016)*, (1), 30. https://doi-org.sunypoly.idm.oclc.org/10.12959/issn.1855-0541.IIASS-2016-no1-art02

Ilievski, A., Bernick, I. (2016). Social-Economic Aspects of Cybercrime. *Innovative Issues and Approaches in Social Sciences, Vol 9, Iss 3 (2016)*, (3). https://doi-org.sunypoly.idm.oclc.org/10.12959/issn.1855-0541.IIASS-2016-no3-art1

Kesari, A., Hoofnagle, C., & McCoy, D. (2017). Deterring Cybercrime: Focus on Intermediaries. *Berkeley Technology Law Journal*, *32*(3), 1093–1134. https://doi-org.sunypoly.idm.oclc.org/10.l5779/Z387M04086

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, *58*, 39–46. https://doi-org.sunypoly.idm.oclc.org/10.1016/j.cose.2015.12.001

Kshetri, N. (2009). Positive Externality, Increasing Returns, and the Rise in Cybercrimes. *Communications of the ACM*, *52*(12), 141–144. https://doi-org.sunypoly.idm.oclc.org/10.1145/1610252.1610288

Leiker, A.R. (2018) Nov 14. Tyler Barriss, who made fatal swatting call in Wichita, guilty of 51 federal charges. *The Wichita Eagle*. Retrieved from https://www.kansas.com/news/local/crime/article221616115.html

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, (3), 287. https://doi-org.sunypoly.idm.oclc.org/10.1007/s10610-016-9332-z

Strikwerda, L. (n.d.). https://doi-org.sunypoly.idm.oclc.org/10.1080/13600834.2014.891870

Urbas, G. (2012). Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement. *Journal of Internet Law*, *16*(1), 1–17. Retrieved from http://sunypoly.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=77467987&site=eds-live

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *CyberPsychology, Behavior & Social Networking*, *20*(7), 407–412. https://doi-org.sunypoly.idm.oclc.org/10.1089/cyber.2017.0028

Zetter, K. (2008, Nov 24). Lori Drew's Daughter 'Devasted' by Friend's Suicide But Doesn't Feel Responsible. *Wired*. Retrieved by https://www.wired.com/2008/11/defendants-daug/

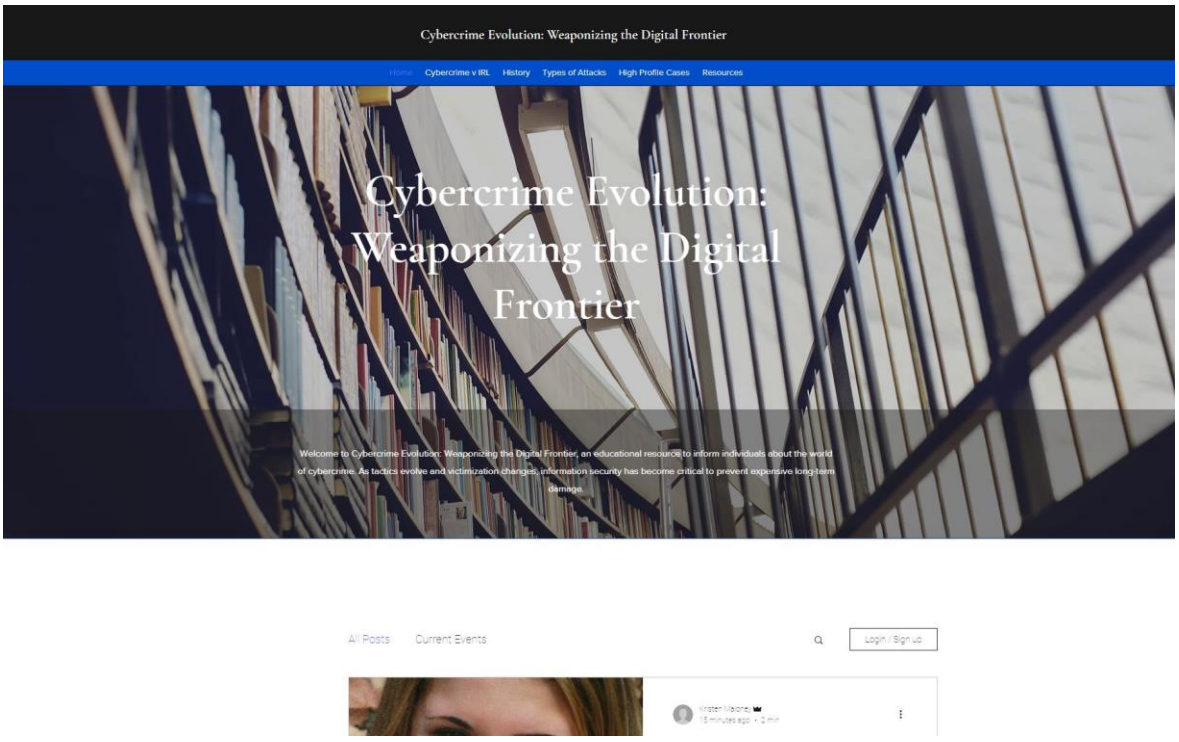

FIGURE 1: SCREENCAP OF HOMEPAGE

FIGURE 2: SCREENCAP OF SECTION: "CYBERCRIME VS. IRL"

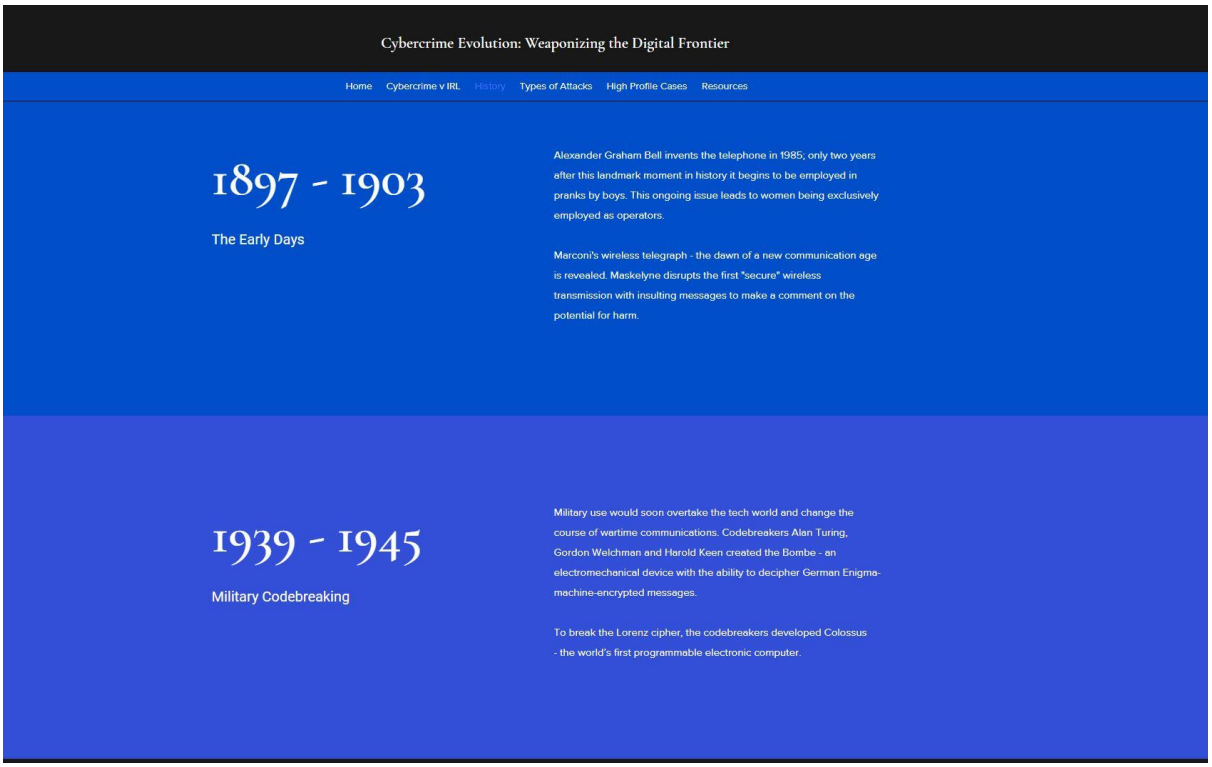

FIGURE 3: SCREENCAP OF SECTION: "HISTORY OF CYBERCRIME"

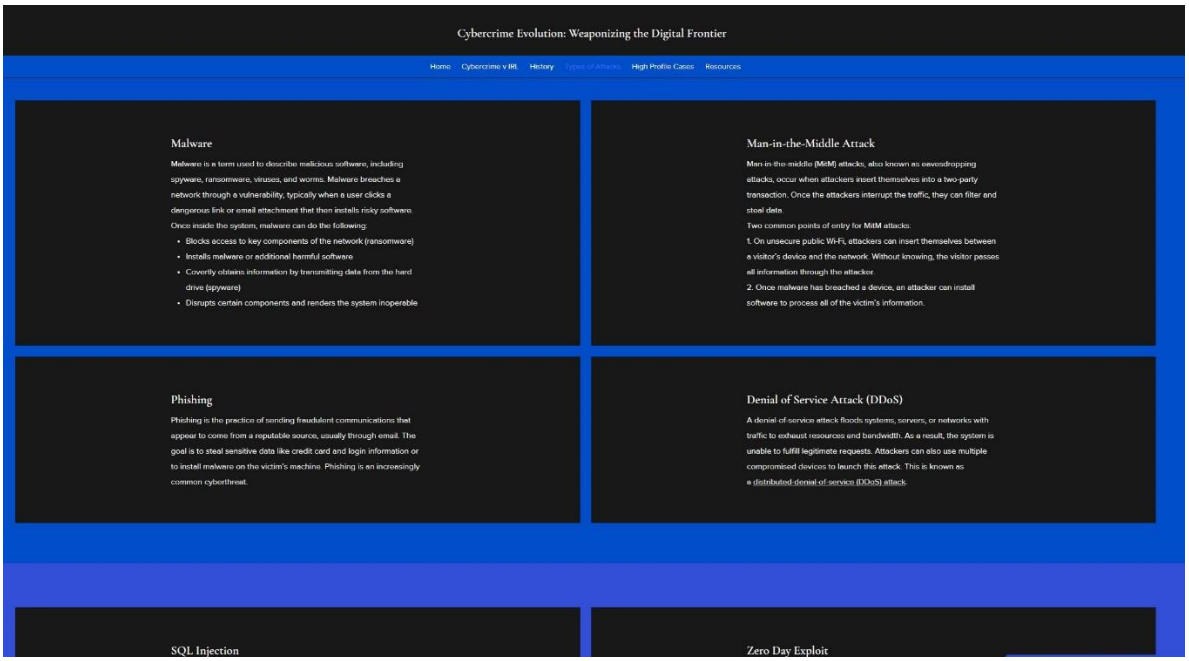

FIGURE 4: SCREENCAP OF SECTION "TYPES OF ATTACKS"

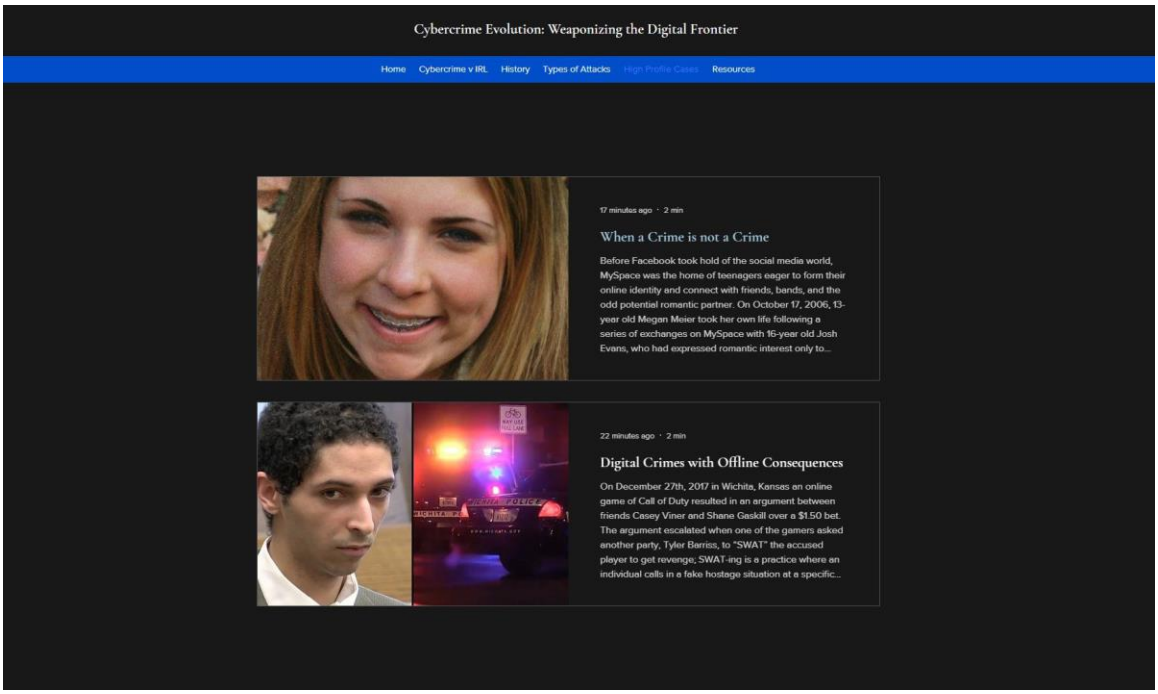

FIGURE 5: SCREENCAP OF SECTION "HIGH PROFILE CASES"

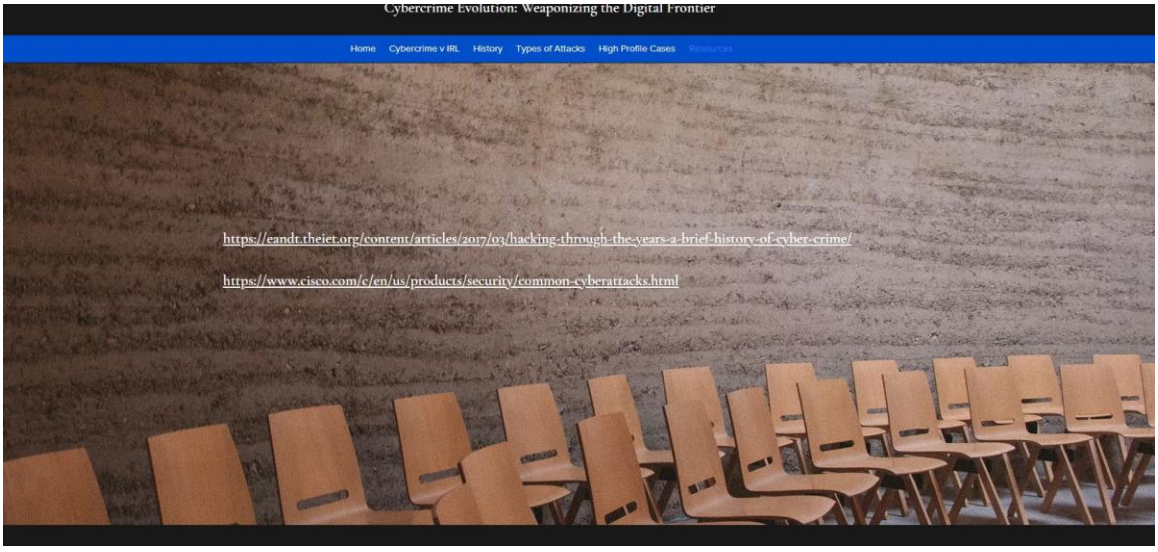

FIGURE 6: SCREENCAP OF "RESOURCES"