Journal of Crime and Criminal Behavior
Vol. 4, No. 1, 2024, pp. 91-112

URL: www.arfjournals.com
https://doi.org/10.47509/JCCB.2024.v04i01.04

Cybercrimes and Safety Policies to Protect Data and Organizations

Bahaudin G. Mujtaba
Nova Southeastern University, 3301 College Avenue, Fort Lauderdale, FL. 33314-7796. USA.
E-mail: mujtaba@nova.edu

TO CITE THIS ARTICLE

Bahaudin G. Mujtaba (2024). Cybercrimes and Safety Policies to Protect Data and Organizations. *Journal of Crime and Criminal Behavior,* 4: 1, pp. 91-112. *https://doi.org/10.47509/JCCB.2024.v04i01.04*

Abstract: Technological developments in cyberspace activities, innovations to keep users online, and the widespread use of online banking or e-commerce shopping have made it easier for cybercriminals to steal one's data, identity, and money in a matter of minutes. Such concerns have also made it a requirement for human resources professionals in today's digital workplace to become aware of modern concerns regarding data handing procedures, while also guarding the entire organization.

This paper provides insights into the world of the dark web where criminals can purposely target, steal, and use other people's personal data and income. Finally, the paper emphasizes that awareness of various phishing techniques and being careful along with clarity and consistency in guarding access and data can help keep individuals and organizations from regularly becoming targets and victims of cybercriminals.

Keywords: Cybercrimes; e-commerce; privacy breach; data security.

Introduction

The widespread existence and fast growth of e-commerce have transformed the modern workplace and society in most developed economies where consumers now have regular access to the internet (Mujtaba and Cavico, 2023). The same applies to opportunistic cybercriminals who are using their internet, technology skills, and security gaps to pray upon anyone and everyone to enrich themselves. Since we are all now experiencing the growth and development stages of the internet and e-commerce along with data breaches, sound legal and practical policies must be continuously created, adapted, and revised as necessary to keep individuals and organizations safe from hackers.

Received : 18 January 2024 • **Revised :** 21 February 2024 • **Accepted :** 02 March 2024 • **Published :** 15 March 2024

Cybercriminals adjust their techniques for stealing information, and so should individuals and institutions in how they guard their valuable networks and privacy data (Sheilds, 2023). While there are similarities, today's cybercriminal does not necessarily fit the profile of a thief or criminal of the past.

Cybercriminals have changed the traditional notion of "only people with personality disorders would commit illegal crimes." Some people have viewed thieves and criminals as "psychopaths" or "sociopaths," terms which refer to the antisocial personality disorders of individuals that have had a pattern of disregard for others' personal data, their right to privacy, and their right to enjoy what belongs to them (Taylor et al., 2019). Generally, characteristics associated with antisocial personality disorder tend to be egocentrism, self-esteem derived from personal power, having no standards of right and wrong, disregarding the wellbeing and feelings of others, being deceitful and hostile, irresponsibility, and/or impulsive risk-taking. While some cybercriminals are likely to fit the profile of a "psychopath" or "sociopath," research shows that "the prevalence of antisocial personality disorder is lower among computer criminals than among other criminals" (Taylor et al., 2019, p. 55). Cybercriminals commit their crimes for a variety of reasons and protection mechanisms must be put in place to guard against all such offenses to protect employees, consumers, and organizations.

Cybercrimes happen locally, nationally, and internationally around the globe and anyone can be a victim. For example, a Turkish citizen by the name of Ercan Findikoglu (otherwise known as "Segate", "Predator" and "Oreon") received an 8-years prison sentence for organizing, leading, and carrying out cyberattacks on the global financial system during the years of 2011 to 2013, which causes losses close to $55 million. In one of their attacks on February 27 of 2011, Findikoglu and his coconspirators stole around $10 million from 15,000 ATM machines through illegal withdrawals in 18 countries (U.S. Department of Justice, 2017). Such incidents create many victims who suffer financial losses, while creating an environment of chaos, fear, and panic for millions that become aware of it through social media, radio, or television news.

A 31-year-old Floridian, Timothy Livingston, residing in Boca Raton, was found guilty of conspiracy to commit fraud in connection with illegally accessing computers, emails, and identity theft (U.S. Department of Justice, 2017). Livingston's crime used stolen emails to generate more than $1.3 million in profits. Along with his conspirators, they were able to send spam to stolen emails while concealing the sender's information and bypassing protection filters. Perhaps money motive was his main goal, regardless of how it was generated. He was sentenced to serve four years in prison. Of course, the question is whether a four-year sentence is a sufficient deterrence to prevent such individuals from future fraud?

One recent headline example is the article entitled, "*FTC Sues Kochava for Selling*

Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations," where the agency charges that the firm's geolocation information from millions of mobile devices can be used to personally identify specific individuals and trace their movements (FTC, August 29, 2022). Apparently, the Federal Trade Commission (FTC) is suing data broker Kochava Inc. for "selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations" (para. 1) that should remain confidential. The public exposure of such personal information could endanger a person or groups of people if they went to the reproductive health clinics, religious organizations such as temples and mosques, violence shelters, and even to addiction or healing services. Given the unfortunate political rhetoric in society, such personal information can have a disparate impact on some minority groups as it can lead to the stigmatization, annoyance, discrimination, job termination, and even bodily harm of innocent individuals in the community (Muffler, Cavico, and Mujtaba, 2010). The FTC lawsuit is attempting to stop companies from selling any sensitive geolocation data and they must be required to immediately and properly delete any such vulnerable information they might have already collected. Of course, the goal of FTC has always been to protect sensitive consumer data, including geolocation and health information of all citizens, from being misused by falling into the hands of criminals (Mujtaba and Cavico, 2023). Sound regulation is necessary to encourage data protection of private citizens and networks that keep our society moving forward each day.

Cybercrime Examples

Headlines are plentiful each week regarding cybercrimes. We will focus on a few that involve individuals, institutions, and governments. Recently, the U.S. government officials were trying to contain the negative impact of the latest leak of classified documents from Pentagon on social media during March and early April 2023. The U.S. Defense Department found out who leaked the sensitive intelligence data.

The suspect of the Pentagon classified military intelligence document leaks was caught by the U.S. authorities. His name is Jack Teixeira, 21 years old, and he was a Massachusetts Air National Guard member. Jack was arrested in his family residence in Dighton, Massachusetts. A member of Jack's online messaging group on Discord reported the source of the document leaks to the FBI. Jack, on April 12, went before Magistrate Judge David Hennessy of the U.S. District Court in Boston, as he was being charged under the Espionage Act. While he was being charged, Jack's father told him, "Love you, Jack!" — and he responded back by saying, "Love you, too, Dad" (Manzhos, Barrett, and Wagner, 2023). Through this illegal leaking of critical data, Jack has now ruined his life and that of his family, perhaps unintentionally, due to his

level of immaturity or lack of sufficient training on the importance of keeping the data confidential.

As mentioned by Taylor, Fritsch, Liederbach, Saylor, and Tafoya (2019, p. 111), espionage has been around for many centuries as basic tradecraft secrets were initially stolen in the 1700s from China by the Europeans so they could more effectively compete with the superior products produced by the Chinese porcelain manufacturing. There is industrial espionage, economic espionage, and corporate espionage. Jack's leakage of the sensitive intelligence documents fit into the economic espionage, which is "the misappropriation of trade secrets with the knowledge or intent that the offense will benefits a foreign government, foreign instrumentality, or foreign agent", which can include "stealing, copying, transmitting, buying, and/or destroying someone else's trade secrets" (Taylor et al., 2019, p. 111). Regardless of whether helping foreign government was Jack's intention or not, the impact is there nonetheless as many adversary governments now know that Americans have tracked their sensitive communications. Of course, such leakage or espionage are considered criminal behavior under the Economic Espionage Act of 1996 (EEA). EEA is the first federal act to define and enforce penalties for trade secrets theft, thereby making it illegal to steal, copy, sketch, download, or communicate such data to others without expressed permission from the owners.

It is surprising that an irresponsible young man, who loved playing games online and being part of the teenage cyber community, was entrusted with such sensitive documents. He held a top-secret clearance for the past two years and was legally allowed to view classified material. He could access the internal Defense Department computer network called the Joint Worldwide Intelligence Communications System, where he could read or print classified documents. Eventually, Jack leaked confidential and classified documents which could jeopardize the lives of people all over the globe. The question is, why would a low-level ranked technology support staffer as a National Guard member, in Massachusetts, have had access to the country's classified and sensitive national and international information at the Pentagon? Of course, there are many low-level ranked individuals that never commit such crimes and serve the country with honor and dignity that can serve as role models for everyone entrusted with sensitive documents. The availability of applications such as ChatGPT and modern artificial intelligence tools will make it more tempting for criminals to commit crimes without being easily detected.

Steve Wozniak (2023), Apple's co-founder with the late Steve Jobs, states that artificial intelligence (AI) has its first word is correct, that computers are artificial, but they are not necessarily intelligent. We call AI programs intelligent, but we don't really know how the brain works. Wazniak warns that AI helps human beings solve complex problems, but it can also be used by scammers and cybercriminals to scam people,

steal data, and commit crimes more intelligently. As such, in the coming years, people, corporations, and governments should become more secure as online scammers are likely to increase their attacks.

An article reported that a mysterious transnational organization made up of cybercrime thieves stole millions of dollars using tampered gift cards (Santora, 2013). Apparently, the bank robbers had encoded bank cards that had no withdrawal limits and were robbing banks through ATM machines. Within a matter of two hours and twenty-five minutes, the robbers covered approximately 750 ATM transactions, stealing thousands of dollars. The crime was not only happening in the state of New York, but also in numerous others in at least 20 different countries around the world simultaneously and during the same days and nights. The organized cybercrime robbed money from 4,500 ATM transactions, in the amount of $5 million in losses. If these large and small banks alike were victims in this case, what chance do the average individual bank account holders have?

Another bank crime took place in Maharashtra, a city in India. This crime was a $14 million ATM Heist through the hacking of ATM machines in multiple countries across the globe. The hackers used VISA's ATM cards that were issued to a bank, in Pune, India. There were more than 20 ATM's that were affected by the heist. The assailants were under the impression that the money that was being withdrawn was for a part in a movie. It was reported that they assumed roles as extras in an elaborate heist, not an actual movie but a fake made up one (Lee, White, and Jones, 2023).

Nowadays, scammers can use applications such as TikTok, Snapchat, and Facebook in their AI schemes to steal personal data. For example, the scammers can take one's post and use his/her image, voice, and location to use for a trip they are planning. Raasch (April 23, 2023) mentions that Jennifer DeStefano was an example of a scam using the artificial intelligence (AI) generated voice of her daughter. The scammers used Mrs. DeStefano's daughter's voice in a scheme of pretending that she was kidnapped, and they were asking for money for her daughter's safety. It was reported that the mother believed that the voice seemed so real that she was scared for her daughter's life. In this scenario, she quickly found out that her daughter was safe and did not fall victim to these scammers. One can only imagine what this mother was going through since scams using the AI-generated voice of her daughter did appear real to her. The idea of one's daughter being kidnapped and the thief's needing money for her daughter's safety is a bit too real as scammer have been doing similar acts using a phone call to the elderly. Many parents who live in Gainesville or other places throughout the United States report having received similar calls several times over the past decade that their son was sick in the hospital and money is needed for blood transfusion. Consequently, many parents now do not answer any phone calls until the caller leaves a message, and

they recognize it. The story shows that modern scammers will go far to steal money from innocent individuals. All social media users must be extra careful and watch what their family members, especially young kids, are posting online. Social media and Al will continue to be used to illegally monitor people in hopes of stealing their personal data for misuse.

The Idaho Community Hospital fell victim to a cyberattack at the end of May 2023. The cyberattack disrupted their computer network and caused the healthcare facility to divert ambulances to other medical facilities. Of course, such attacks mean "life or death" for urgent emergency cases or patients that need immediate care or constant care. This unfortunate cyber-attack caused medical professionals and staff to rely on the use of pen and paper to take care of their patients (Lyngaas, 2023). It is very possible that some healthcare facilities are quietly paying ransom to hackers and not reporting them which means the problem continues as more and more unsuspecting facilities become victims.

The good news is that leaders around the world are all realizing that they need to cooperate to root out cybercrimes. As a matter of fact, a British citizen was extradited and pleaded guilty to cybercrime offenses. Joseph James O'Connor, a/k/a "PlugwalkJoe," on April 26, 2023, was extradited from Spain and pleaded guilty before U.S. District Judge Jed S. Rakoff to charges which included (British Citizen Extradited, 2023):

1. Conspiracy to carry out computer hacking along with his co-accusers to utilize a digital interruption strategy known as a SIM trade assault to take thousands of cryptographic monies from a Manhattan-based digital money organization.
2. PC interruptions connected with takeovers of TikTok and Snapchat client accounts and cyberstalking two separate victims.

Apparently, Joseph used his sophisticated technological skills for malicious purposes to conduct a complex SIM swap attack to steal cryptocurrency, hacking Twitter, conducting computer intrusions to take over social media accounts, and even cyberstalking victims, including a minor child. This conviction shows that law enforcement leaders are joining hands to punish those who victimize others through cyber-attacks in a flagrant, intentional, and malicious manner. Joseph harassed, threatened, and extorted many of his innocent victims, causing them and their family members substantial emotional harm and distress. He was able to stay anonymous using his computer skills to hide behind secret accounts and aliases. It is great to see that global leaders, investigators and prosecutors can identify, locate, extradite, charge, and bring to justice such local and global criminals to ensure they face the consequences for their crimes in a timely manner.

Criminology Theories

Criminology's choice theory emphasizes that people often commit a crime consciously, intentionally, and through proper planning, sometimes as a solo act and at other times with co-conspirators that have similar goals. These criminals do know the benefits and costs associated with the crime, where severe penalties can serve as a deterrence for some actions, while great rewards can be financial or symbolic in terms of name recognition for being the best hacker in the field (Taylor, Fritsch, Liederbach, Saylor, and Tafoya, 2019, p. 49). According to Taylor and colleagues (2019), the choice theory became popular among criminologists in the 1970s because crimes had significantly increased in the prior decade. The positive school (belief that crime-producing traits could be isolated and controlled) began to be questioned, and because rehabilitation practices were under attack since reports had showed that they had little to no appreciable effect on the rates of recidivism. Overall,

> Choice theory argues that since the offender has made a rational choice to commit the offense, the focus should be on the offense committed, not the offender. Policies such as mandatory sentencing and "three strikes and you're out laws" are popular and are based on choice theory. The idea is that the way to control crime, including cybercrime, is to have offenders fear the punishment and be deterred from committing the act. Since humans are hedonistic, efforts should be placed on making the risks of committing cybercrime higher than any benefit derived from committing the offenses (Taylor et al., 2019, p. 50).

Supporters of the punishment for deterrence of cybercrimes are under the assumption that offenders consciously weigh the risks and benefits and would not commit the crime if the risks are greater than the benefits. Of course, the reality is that many criminals continue to repeat illegal offenses despite having been punished for prior acts. Reports have consistently shown a significant rate of recidivism for many that have served time in the American prisons. As such, the idea of more severe punishment does not always deter wrongdoings, especially for white-collar crimes (such as data breaches, tax fraud, insider trading, medical fraud, insurance fraud, bribery of low-level officials, embezzlement, money laundering, hacking into computers, etc.). Therefore, one must study other theories and practices in search of better answers.

Lawrence Cohen and Marcus Felson (1979) explain that motivation, vulnerability of targets, and lack of sufficient security play a huge role in the frequency of cybercrimes which they discuss in the "routine activities theory." The "routine activities theory" claims that there will always be a steady suppliers of people motivated to commit crimes since changes in crime rates are associated with changes in the availability of possible victims that lack sufficient security precautions. Consequently, "when motivated offenders

are present, they make rational choices by selecting suitable targets that lack capable guardianship" (Taylor et al., 2019, p. 51).

According to Holt and Bossler (2009), the routine activities theory supports the increase of online harassment since going online has now become the norm through the availability of computers and smartphones that are always connected to cyberspace. Research shows that being engaged in online forums on regular basis, connecting with deviant peers, and committing illegal activities do expose people to skilled offenders, thereby increasing a person's chances of becoming a victim. More specifically, "Individuals engaging in media piracy and viewing pornography were at an increased risk of malware infection, largely because these files are attractive packages that many individuals would want to open" (Holt and Bossler, 2009; Taylor et al., 2019, p. 51).

Experts on the "differential learning theory" explain that criminal behavior is learned and repeated, not necessarily because a person cannot obtain economic success through other means. For example, Sutherland and Cressey (1978) offer several propositions which emphasize the social interactions and learning can lead to illegal actions:

1. Criminal behavior is learned through observation and is not due to biological or psychological traits.
2. Criminal behavior is learned through interactions and communications with others.
3. Criminal behavior takes place through intimate personal groups.
4. Criminal behavior is learned through techniques of committing such acts, and having specific directions, motives, and rationalization for it.
5. Criminal behavior and motives are learned by associating with people who believe legal codes should be broken.
6. Criminal behavior is strengthened when one is associated with more people who favor violation of the law.

Sutherland mentions that differential associations can vary in frequency, duration, priority, and intensity. Furthermore, learning criminal behavior is very similar to learning to drive carefully and doing well in school. Finally, having a need for money or economic success is not a valid explanation for criminal behavior since workers legally work to obtain money, and thieves illegally steal to acquire money. Having a need for money and psychological success can be explained by lawful and unlawful behaviors (Sutherland and Cressey, 1978; Taylor et al., 2019, p. 61-62).

Recommendations

Internet and the social media technologies and applications have advanced faster than the laws about their ethical and legal use. Social media is vast, and can include social or

professional networking, blogs and micro-blogs, digital media video and image sharing, and other online applications which may include location-sharing, consumer reviews, virtual worlds, and social bookmarking (social media, 2018). Businesses and government officials must do everything possible to protect employees and consumers. Moreover, employees and customers must also be educated to take personal responsibility in cautiously posting and sharing their personal data (Wilkinson & Reinhardt, 2015).

Most technically savvy organizations are putting social media into good use by promoting their firms' brand awareness and by regularly engaging their customers; in this way, this constant social media engagement allows firms to "keep their finger on the pulse" of their existing and prospective clients and customers. Some of the most common social media usages and practices can include (Social Media Risks, 2019) correcting rumors and false information that are hurtful to one's image and brand. In addition, proper social media use is often associated with employment practices, such as the staffing, attraction, and retention of workers.

Companies need to educate their employees about ethical decisions that are good for employees, consumers, and society in general (Cavico and Mujtaba, 2016). Otherwise, regulations will be imposed by the government sector to legally punish real and perceived unethical violators.

Technical errors and personal data of employees or consumers being stolen can take place at the most secured facilities via network vulnerabilities. For example, during August 3, 2022, Equifax admitted that some consumer credit scores were changed mistakenly because of their computer problems. Apparently, according to the company, a server "coding issue" was the cause of the inaccurate scores. Earlier, it had been reported that Equifax gave inaccurate credit scores for millions of American consumers that were securing loans. Incorrect scores were sent about these consumers around March-April until they became aware of it or revealed this problem in May of 2022. Prior to this, there was a cyberattack at Equifax, and hackers had accessed Social Security numbers, driver's license numbers, and home addresses of their consumers (Saharan, 2022). If the disclosure of consumers' identifiable information become widespread and the norm for some firms, then even the company's officials can be fined by the government for not properly securing private data. Moreover, the company will be sued civilly for invasion of privacy for negligence and perhaps even gross negligence, thus risking punitive damages for the latter culpability.

Retain the Top Talent

Modern technologies and regulations should all be balanced to help companies successfully serve their constituencies. If the public sector laws are too strict, it will stifle creativity in any capitalistic marketplace and create distress for employers, workers, and

customers. If there are no laws, then some "greedy" and overly ambitious managers will focus on maximizing their profits at the cost of undue risks to personal data of their employees and customers. Again, reference must be made to the infamous Wells Fargo fake account and hacking scandal (Cavico and Mujtaba, 2017). Therefore, there should be a balance of sound legal regulations and organizational ethical policies to have a high level of trust and confidence among clients, customers, employees, managers, organizations, government regulators, and the legal profession.

Attracting and retaining employees in this changing time of post-Covid-19 pandemic recovery times is one challenging and complicated task, but certainly a necessity always for great managers and firms that want to make a positive difference for their employees, community, stockholders, and other stakeholders, including society.

It is very important to take the time necessary to clearly communicate these policies and programs, particularly the privacy policies, with all workers through the company's ethics code, manual or handbook, training programs, blogs, website, and other platforms, and especially before these policies are implemented and enforced. As always, it is essential to note that change can be difficult for employees; so, the firm should remain open-minded, listen to any concerns, and professionally and proactively discuss any potential issues, especially regarding data privacy. Of course, if used properly, the use of modern technologies can be a very powerful tool to boost productivity, safety, security, and collegiality in the workplace (Blaisdell, 2021, para. 7).

Equal Access is no Longer!

While there are criminals that purposely plan to illegally access computers and bank accounts, others have policies that lead to a negative or disparate impact on some populations. Nowadays, for example, there are ethical concerns regarding access and the power of service providers to control the speed of their members. Grimmelmann (2019) explains that "network neutrality" rules require internet service providers (ISPs) to provide equal access to their networks to all subscribers. In other words, Internet speeds should not be slowed down indiscriminately since everyone has the right to equal access to the modern digital diversity that exists in the online world (Ohlhausen, 2013). Some people use the term "Internet freedom" to describe "net neutrality." Such issues and privacy concerns merit awareness, reflection, as well as integration into discussions regarding regulations impacting e-commerce along with the quality engagement of employees in the organization (Phomkamin et al., 2021). As mentioned by Ohlhausen (2013, p. 81): "Some content providers want the government to adopt regulations to guarantee them fair access to the Internet," however "some network owners, like Verizon or Comcast, disagree and think such regulations are unnecessary and could stifle innovation on the Internet." Of course, such debates will continue to

take place among consumers, businesses, and government officials because these are the times of transformational change that will determine how we access and use the Internet over the coming years, decades, and century. Hopefully, all internet links can be accessed more safely in the future without having to worry about being illegally hacked or indiscriminately slowed down.

Privacy is no Longer!

Technology and the widespread use of the internet through social media platforms have reduced privacy as every transaction provides an opportunity for personal data to be stored on "cookies" or leaked to unethical users or criminals. In the modern society, we see that hackers and law enforcement officials alike can easily access anyone's computer, phone contacts, text messages, and call-history from mobile devices without the person's permission and without notice. While there are conveniences associated with technology, there certainly are negatives as well. As human beings progress, move forward, take on new initiatives, and invent better or more intrusive technologies, the legal side of protecting people's rights must also keep pace with it simultaneously. As such,

> This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature (Warren and Brandeis, 1890, p. 194).

When private data are intentionally or unintentionally stolen or leaked, the transmission can cause "emotional harm," especially on impressionable young teenagers. On June 29, 2022, PBS News in South Florida discussed mental health and how more young people have been thinking of committing suicide because of conflicting information, lack of sufficient mental help counseling, and the additional challenges associated with Covid-19 isolation over the past three years in the United States of America. In 2022 alone, nearly 50,000 Americans committed suicide. Human resources professionals can and should educate employees and warn them about privacy rights and responsibilities and social media risks regarding personal data as well as to educate everyone on how to protect their own privacy and that of their colleagues' and customers, particularly by not publishing any private information on public forums.

While all firms must be concerned about the data and privacy of their employees, vendors, suppliers, and customers, this awareness is especially true for e-commerce-

linked firms since trust is essential for their existence. As human resource professionals and managers, we must all be concerned about the ubiquitous nature of modern technology, the prevalence of cybercriminals as well privacy issues and concerns, and the utmost importance of keeping employees' as well as customers' data secure.

Through the internet, both small and large-scale entrepreneurs can capitalize on new business opportunities more easily by accessing highly segmented customers worldwide in just a matter of days, if not hours, through email distribution or website promotions (Phomkamin et al., 2021).

Most experts agree that "The genius and explosive success of the Internet can be attributed in part to its decentralized nature (sector-based laws) and to its tradition of bottom-up governance" (Clinton and Gore, 1997, p. 4). The decentralized framework enables and empowers creative entrepreneurs to capitalize on their innovations, hard work and persistency in meeting specific consumer needs locally, nationally, and globally. Similarly, cybercriminals can take advantage of the relaxed environment and easily hack into people's private files and steal from them.

Trust is no longer a Given!

Research shows that companies have a moral and legal responsibility to protect personal data provided by consumers. To make sure firms are protecting data, the government has stepped up by creating agreed-upon common sense laws. As a matter of fact, the Consumer Privacy Bill of Rights, in the United States, "applies to *personal data*, which means any data, including aggregations of data, which is linkable to a specific individual…Personal data may include data that is linked to a specific computer or other device" (Consumer Data Privacy, 2012). It should be clear to all managers and organizations that consumers must be able to exercise "individual control" over all the personal data companies collect from them and how that data is being used.

Furthermore, besides allowing individual control to consumers over the collection and usage of their personal data, there should also be transparency, respect for context, security, fair access, accuracy, focused collection, and full accountability to enforcement authorities, consumers and clients for alignment and adherence to all the stated legal and ethical principles. Human resource professionals and managers must be aware of another old maxim: "Once your reputation for integrity is lost, it is very difficult to get it back," as shown from the Wells Fargo bank fake account and hacking scandal (Cavico and Mujtaba, 2017).

The Federal Trade Commission provides relevant guidance for all firms on data privacy as they work "for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them" (Children's Online Privacy Protection Rule, 2000, p. 15).

FTC's guidelines and recommendations can be used for learning, assessment, and policy development at the organizational levels. The expectation is that organizations must train their managers and workers on how to properly handle personal data while regularly assessing their performance to make sure there are no violations of privacy rights. Furthermore, companies should conduct regular or annual audits to evaluate the performance of their managers and employees regarding the protection of personal data from their consumers. Also, any disclosure of personal data to third parties must guarantee that the beneficiaries "are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise (Consumer Data Privacy, 2012, p. 48).

There are many practical and specific rules provided by the FTC for online privacy protection, including "*How to Comply with Children's Online Privacy Protection Rule*" which is of interest to parents since teenage children often share personal data online. Of course, individuals, companies and government policies must all work together simultaneously toward the same goal of keeping children safe. Since most citizens are not likely to be able to change government policies on their own, then individual control and company responsibility should be emphasized regularly to create awareness and immediate protection for data security. However, each citizen should, and must, exercise his/her right during the election process by voting for those candidates who will represent their collective views at the government level so certain data, especially pertaining to young children can, remain private.

At a minimum, all managers and human resource professionals must know and adhere to the Children's Online Privacy Protection Act, which became effective April 21, 2000, because it applies to the online collection of adolescence's personal and identifiable information if they are under 13 years of age. In general, everyone must remember that "It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed" by the Federal Trade Commission (Children's Online Privacy Protection Rule, 2000, p. 7). Ultimately, it is the consumers who are in the best position to secure and safeguard their own personal data, while also demanding protection by firms.

Create Awareness about Phishing Techniques

Criminals use many tools to get your data using legal and illegal means such as asking for it through various means, sometimes through practices such as phishing, spear phishing, and whaling.

Phishing is a type of social engineering technique criminals use to attack and steal user data. If you are ever hacked with phishing, you have a high chance of losing your

login information, credit card numbers, and other such important private data that you do not want others to see. People who have been 'phished' are most often baited through text messages, emails, instant messaging, and even those annoying pop-up ads.

Spear phishing tends to be semi-targeted and describes a situation when a group or individual attacks a "specific" organization or individual by sending them a false or scam email. The email usually looks like it is coming from a legitimate or reputable source but is malicious and full of harmful malware that infects one's computer. In such spear phishing techniques, criminals steal information such as banking details and data from their employees, consumers, and other victims.

The *whaling* form of phishing tends to be highly targeted toward high-level executives and influential candidates. It is a form of email attack, but instead of sending these attacks to normal individuals, it is aimed at attacking anyone who is seen as "high-profile" such as chief executive officers (CEOs) of large corporations, politicians and even celebrities. Tips to avoid phishing in the modern workplace, managers must create awareness of such hacking possibilities and do some or all the following which are recommended by experts:

1. Educate yourself and all your employees, key vendors, and customers about online fraud and how to identify phishing emails.
2. Flag all suspicious emails that come from outside the organization.
3. Discuss the use of social media with the executive teams as it relates to phishing.
4. Establish a multi-step verification process for all requests for sensitive data or wire transfers.
5. Exercise data protection and data security policies.
6. Know that emails which demand "fast" action, that they might be a scam as people who sent the emails often count on the recipients to respond quickly, before anyone notices that it is a scam.
7. Emails with spelling mistakes or grammar errors can be a red flag for employees to look out for as it might be a scam.
8. Look for things that do not match; for example, the logos, domain names and email addresses which might be slightly different. If something looks suspicious, then don't respond as email is probably fraudulent.

Consumer Protection must Be Planned

The Consumer Financial Protection Bureau (CFPB) is a public sector agency in the United States dedicated to making sure Americans are treated fairly by entities such as banks, lenders, and other such institutions. Their aim is to "protect consumers from

unfair, deceptive, or abusive practices and take action against companies that break the law" (CFPB, 2022, para. 3). CFPB (2022, para. 3 - 4) promises to empower consumers, enforce the federal laws, and educate organizations to conduct business in a socially responsible manner.

- *Empower*. CFPB creates tools, answers common questions, and provides tips that help consumers navigate their financial choices and shop for the deal that works best for them.
- *Enforce*. CFPB acts against predatory companies and practices that violate the law and have already returned billions of dollars to harmed consumers.
- *Educate*. CFPB encourages financial education and capability from childhood through retirement, publish research, and educate financial companies about their responsibilities.

The Federal Trade Commission (FTC) is an independent bureau or organization in the United States to enforce the civil U.S. antitrust laws and to protect consumers from fraudulent business transactions. More specifically, the agency's role in any form of commerce is critically significant and very important as "The Federal Trade Commission works to prevent fraudulent, deceptive, and unfair business practices. They also provide information to help consumers spot, stop, and avoid scams and fraud" (FTC, 2022, para. 1).

There are millions of identity theft victims each year in the U.S. As such, one of the main goals of the FTC is to prevent identity theft which hurts consumers' confidence in doing business face-to-face and especially online, where data and information can be collected using "cookies" on each website. When this data is not kept private and not protected well, a person can fall victim to identity theft. Of course, identity theft is a crime. The Identity Theft Act (ITA) sees identification of a person by such element as a name, social security number, date of birth, government-issued driver's license, and biometric data such as fingerprints, etc.

The FTC's Fair Information Practice Principles (FIPP) serve as a framework to protect the privacy of everyone regarding personally identifiable information (PII) at the Department of Homeland Security (DHS). FIPP are recommended guidelines regarding fair and ethical information practices in today's world of electronic commerce or e-marketplace. Many of these principles, if not all, are very relevant for application in any organization today since all firms and individuals are likely to be connected to the internet much of the day in getting their work done. There are eight specific principles to FIPP:

1. Transparency
2. Individual participation

3. Purpose specification
4. Data minimization
5. Use limitation
6. Data quality and integrity
7. Security
8. Accountability and auditing

The security principle of FIPP states that the technology used within the department must be of sufficient quality to ensure private contents or personally identifiable information (PII) are kept secure. The security principle should be practiced by all firms because privacy mandates are supposed to be proactively built into the systems to safeguard employees and consumers' data "from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction." Furthermore, the employed professionals working with PII are required to be certified with relevant qualifications and security standards.

The data minimization principle is there to encourage the collection of only the most relevant information from everyone. The individual choice principle should allow "users" to consent for the collection, use, dissemination, and maintenance of their personally identifiable information. This principle should be practiced by all organizations, including government organizations, and the later must allow and enable individuals to correct any errors through the Freedom of Information Act (FOIA).

While the world of Internet of Things (IoT) is constantly changing everything we do, and consequently more data will continue to be collected for the benefit of consumers and society, the specific principles to keep data secure will need to be adjusted and expanded on in accordance with prevailing legal, ethical, and business norms. In the current times, the utilization of these FIPP guidelines can afford the minimum security needed to keep consumers' data secure in today's cyberspace or Internet of Things world where everything appears to be connected and communicating to something else in real time with the aim of network neutrality or equal access to all.

Summary

Criminal behavior among cybercriminals appears to be based on similar motives as any other criminal, as some want more financial security while others simply want to become the most skilled hackers. Many criminals commit fraud because of a purposeful rational choice and little or no severe consequences. Regardless of the motive, all such activities as piracy, hacking, cyberstalking, and harassment are illegal and must be guarded against by individuals, organizations, and governments.

With the integration of modern technology in this hyperlocal, yet global, and hyperconnected and complex work environment, employers must do everything they legally, ethically, and practically can do to protect their employees, customers, and business operations.

Human resources professional also must educate employees and warn them about all applicable government regulations and practical protocols to protect their own privacy as well as those of their colleagues and clients and customers by not publishing their personal information on social media since everything has the possibility of becoming public in today's age of internet. Therefore, managers and human resources professionals need to make sure the firm's confidentiality, privacy, internet, and cybersecurity policies and practices are legal and moral and are respectful to all stakeholders. Moreover, such policies and practices must not be unduly intrusive or invasive on the day-to-day personal and private activities and interactions of employees, vendors, and customers.

References

Alibeigi, A. Munir, A. B., and Asemi, A. (2022). A decade after the Personal Data Protection Act 2010 (PDPA): Compliance of communications companies with the notice and choice principle. *Journal of Data Protection & Privacy*, 5(2), 119-137. Website: https://www.henrystewartpublications.com/jdpp

British Citizen Extradited (May 9, 2023). *U.K. citizen Extradited and Pleads guilty to Cybercrime Offenses.* The United States Justice Department – U.S. Attorney's Office for the Southern District of New York. Contact person: Nicholas Biase at (212) 637-2600. Link: https://www.justice.gov/usao-sdny/pr/uk-citizen-extradited-and-pleads-guilty-cybercrime-offenses

Cavico, F. J. and Mujtaba, B. G. (2016). Insider Trading v. Trading on Inside Information: A Primer for Management. *European Journal of Business and Management*, 8(17): 72-85. Link: http://iiste.org/Journals/index.php/EJBM

Cavico, F. J. and Mujtaba, B. G. (2020). *Business Law for the Entrepreneur and Manager (4th edition)*. ILEAD Academy: Florida.

Cavico, F. J. and Mujtaba, B. G. (2017). Wells Fargo's Fake Accounts Scandal and its Legal and Ethical Implications for Management. *Advanced Management Journal*, 82(2), 4-19.

Cavico, F. J. and Mujtaba, B. G. (2016). *Developing a Legal, Ethical, and Socially Responsible Mindset for Sustainable Leadership*. ILEAD Academy: Florida.

CFPB (n.d.). *Consumer Financial Protection Bureau: The Bureau.* Accessed on August 27, 2022 at: https://www.consumerfinance.gov/ / https://www.consumerfinance.gov/about-us/the-bureau/

Children's Online Privacy Protection Rule (2000) How to Comply with The Children's Online Privacy Protection Rule: A Guide from the Federal Trade Commission the Direct Marketing Association and the Internet Alliance. Accessed on August 26, 2022, from: https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211appb0823071.pdf

Clinton, W. J. and Gore, A. (July 1, 1997). *The Framework for Global Electronic Commerce*. Clinton Whitehouse: Washington, D.C. Source: https://clintonwhitehouse4.archives.gov/WH/New/Commerce/

Cohen, Zachary, Bertrand, Natasha, and Atwood, Kylie (April 11, 2023). What we know about the major Pentagon intelligence leak. *CNN Politics*. Link: https://www.cnn.com/2023/04/10/politics/classified-documents-leak-explainer/index.html

Cohen, L. and Felson, M. (1979). Social change and crime rate trends: a Routine Activities Approach. *American Sociological Review*, 44, 588-608.

Consumer Data Privacy (February 2012). Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in The Global Digital Economy. *The White House: Washington*. Link: file:///C:/Users/mujtaba/Downloads/The%20Consumer%20Privacy%20Bill%20of%20Rights.pdf

Department of Homeland Security (DHS). Link: www.dhs.gov/privacy

Dot Com Disclosure (2022). *FTC Staff Revises Online Advertising Disclosure Guidelines*. Link: https://www.ftc.gov/news-events/news/press-releases/2013/03/ftc-staff-revises-online-advertising-disclosure-guidelines

Fair Information Practice Principles (FIPP) (December 29, 2008). *FIPP Fact Sheet*. Department of Homeland Security (DHS). Link: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles

FTC (August 29, 2022). FTC *Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*. Federal Trade Commission: Protecting America's Consumers. Link: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

FTC (2022). Link: https://www.usa.gov/federal-agencies/federal-trade-commission

FTC (2017). Privacy & Data Security. Federal Trade Commission: United States of America. Link: file:///C:/Users/mujtaba/Downloads/privacy_and_data_security_update_2017.pdf

Ekran Systems (March 31, 202). *How to Monitor Employees at Work: 7 Best Practices*. Category: Security. Link: https://www.ekransystem.com/en/blog/best-practices-how-monitor-employees-work

European Commission Factsheet (2014). *Factsheet on the "Right to be Forgotten" Ruling*. C-131/12. Link: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/06/factsheet_data_protection_en.pdf

Garon, Jon M. (2020). *A Short & Happy Guide to Privacy and Cybersecurity Law*. West Academic Publishing. Link: https://subscription.westacademic.com/Book/Detail/26942 or at Amazon: https://www.amazon.com/Short-Happy-Privacy-Cybersecurity-Guides-ebook/dp/B08BG6GX93/ref=sr_1_1?crid=2AHPI2W9WSVOC &keywords=A+Short+%26+Happy+Guide+to+Privacy+and+Cybersecurity+Law&qid=1657037170&sprefix=a+short+%26+happy+guide+to+privacy+and+cybersecurity+law%2Caps%2C419&sr=8-1&asin=B08BG6GX93&revisionId=609498bc&format=1&depth=1

GDPR (2014). *General Data Protection Regulation*. Link: https://gdpr.eu/right-to-be-forgotten/

Goitein, Elizabeth (October 22, 2019). How the FBI Violated the Privacy Rights of Tens of Thousands of Americans. Brennan Center for Justice. Link: https://www.brennancenter.org/our-work/analysis-opinion/how-fbi-violated-privacy-rights-tens-thousands-americans

Grimmelmann, James (2019). *Internet Law: Cases and Problems*, 9th edition. Semaphore Press: Middletown: Delaware.

Habinsky, Jason and Boone, Haynes (2022). Monitoring and Protecting Employee Privacy. LexisNexis: *XpertHR Employment Law Manual, 2154.*

Holt, T. J. and Bossler, R. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25.

Hsu, Shih-Yi and Mujtaba, B. G. (2007). Team transformational leadership, trust, satisfaction, and commitment: the testing of a structural equation model in software development teams. *Review of Business Information Systems*, 11(3), 17-28.

IBM (April 16, 2018). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security. *CISION PR Newswire*. Link: https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html

Identity Theft (2022). *Federal Trade Commission: Identity Theft*. Link: https://www.identitytheft.gov/#/

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: it's complicated. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-15).

Jones, C. and Mujtaba, B. G. (2006). Is Your Information At Risk? Information Technology Leaders' Thoughts about the Impact of Cybercrime on Competitive Advantage. *Review of Business Information Systems*, 10(2), 7-20.

Justice Department (2020). *Overview of the Privacy Act: 2020 Edition. Criminal Penalties.* The U.S. Department of Justice. Link: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/criminal#:~:text=The%20Privacy%20Act%20allows%20for,if%20the%20official%20acts%20willfully

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 61-70).

Lee, Jean, White, Geoff and Jones, Viv (April 1, 2023). Lazarus Heist: The intercontinental ATM theft that netted $14m in two hours - BBC News. *BBC World Service.* Link: https://www.bbc.com/news/world-65130220

Lyngaas, Sean (Wed May 31, 2023). Cyberattack forces Idaho hospital to send ambulances elsewhere. CNN Politics. Link: https://www.cnn.com/2023/05/31/politics/idaho-hospital-cyberattack/index.html

Manzhos, Mariya, Barrett, Devlin and Wagner, John (April 14, 2023). THE DISCORD LEAKS: Suspect charged in case involving leaked classified military documents. *The Washington Post*.

Link: https://www.washingtonpost.com/national-security/2023/04/14/jack-teixeira-military-leaks-court-appearance/

McKeon, J. (2022). Meta Faces Another Lawsuit Over Health Data Privacy Practices. *Health IT Security*. Retrieved from https://healthitsecurity.com/news/meta-faces-another-lawsuit-over-health-data-privacy-practices

Muffler, Stephen C., Cavico, Frank J., and Mujtaba, Bahaudin G. (2010). Diversity, Disparate Impact, and Ethics in Business: Implications of the New Haven Firefighters' Case and the Supreme Court's *Ricci v. DeStefano* Decision. *Advanced Management Journal*, 75(3), 11-19.

Mujtaba, B. G. (2003). Ethical Implications of Employee Monitoring: What Leaders Should to Consider! *Journal of Applied Management and Entrepreneurship,* 8(3), 22-47.

Mujtaba, B. G. (2014). *Managerial Skills and Practices for Global Leadership*. ILEAD Academy: Florida.

Mujtaba, B.G. (2022a). Workplace Management Lessons on Employee Recruitment Challenges, Furloughs, and Layoffs during the Covid-19 Pandemic. *Journal of Human Resource and Sustainability Studies*, 10(1), 13-29. DOI: 10.4236/jhrss.2022.101002

Mujtaba, B. G. (2022b). *Workforce Diversity Management: Inclusion and Equity Challenges, Competencies and Strategies (3rd edition).* ILEAD Academy: Florida.

Mujtaba, B. G. and Cavico, F. J. (2023). E-Commerce and Social Media Policies in the Digital Age: Legal Analysis and Recommendations for Management. *Journal of Entrepreneurship and Business Venturing,* 3(1), 119-146. Link: https://doi.org/10.56536/jebv.v3i1.37 ; http://jebv.pk/index.php/JEBV/article/view/37

Mujtaba, B. G. and Kaifi, B. A. (April 2023). Safety Audit Considerations for a Healthy Workplace that Puts "People Before Profit" and OSHA Compliance. *Health Economics and Management Review, 4*(1), 11-25. Link: https://doi.org/10.21272/hem.2023.1-02 / https://armgpublishing.com/journals/hem/volume-4-issue-1/article-2/

Mujtaba, B. and McFarlane, A.D. (Summer 2005). Traditional and Virtual Performance Management Functions in the Age of Information Technology. *The Review of Business Information Systems,* 9(3), 53-64.

Ohlhausen, Maureen K. (February 1, 2013). Net Neutrality vs. Net Reality: Why an Evidence-Based Approach to Enforcement, and Not More Regulation, Could Protect Innovation on the Web. *Engage*, 14(1), 81-87. Available at SSRN: https://ssrn.com/abstract=2670816 ; Link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2670816

Phomkamin, J., Pumpuang, C., Potijak, P., Sangngam, S., Ketprasit, I., and Mujtaba, B.G. (December 2021). Engagement Strategies for E-commerce Businesses in the Modern Online World. *SocioEconomic Challenges, 5*(4), 24-34. Link: https://armgpublishing.sumdu.edu.ua/journals/sec/volume-5-issue-4/article-2/

Raasch, Jon Michael (April 23, 2023). How scammers are using your Snapchat and TikTok posts in their AI schemes. *Fox News.* Link: https://www.foxnews.com/tech/scammers-are-using-your-snapchat-and-tiktok-posts-in-their-ai-schemes

Rustad, M. L. & Koenig, T. H. (2019). Towards a global data privacy standard. *Florida Law Review*, *71*, 365. Link: http://www.floridalawreview.com/2019/towards-a-global-data-privacy-standard/

Sadiq, U., Khan, A. F., Ikhlaq, K., and Mujtaba, B. G. (June 2012). The Impact of Information Systems on the Performance of Human Resources Department. *Journal of Business Studies Quarterly,* 3(4), *77-91*. Available at: www.jbsq.org

Saharan, Shubham (August 2, 2022). Equifax Says Consumer Credit Scores Changed in Computer Error. *Bloomberg: US Edition.* Link: https://www.bloomberg.com/news/articles/2022-08-02/equifax-says-consumer-credit-scores-changed-by-computer-error

Santora, Marc (May 9, 2013). In Hours, Thieves took $45 Million in ATM Scheme. https://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?smid=url-share

Shields, Tomothy (April 2023). *MLAW 3006 - Cyber and Information Crimes.* Shepherd Broad College of Law: Nova Southeastern University.

Solove, Daniel (Nov. 13, 2015). The Growing Problems with the Sectoral Approach to Privacy Law. Privacy + Security Blog: Teach Privacy. Link: https://teachprivacy.com/problems-sectoral-approach-privacy-law/

Social Media (2018). *Social Media in the Hiring Process*. Practical Law Practice: Note 9-535-2907. Westlaw: Thomson Reuters.

Social Media Risks (2019). *Social Media Risks and Rewards*. Practical Law Practice: Note 8-501-1933. Westlaw: Thomson Reuters.

Sutherland, E. H. and Cressey, Dr. R. (1978). *Criminology*, 10th edition. J.B. Lippincott Co.: Philadelphia.

Tansey, C. (2022, January 25). *4 ways HR teams can address inflation*. Lattice: Resources for Humans. Retrieved August 25, 2022, from: https://lattice.com/library/4-ways-hr-teams-can-address-inflation

Taylor, R., Fritsch, E., Liederbach, J., Saylor, M., and Tafoya, W. (2019). *Cyber Crime and Cyber Terrorism*, 4th edition. United Kingdom: Pearson.

Telecommuting (2022). *Telecommuting Policies: Key Drafting Tips*. LexisNexis. Accessed August 1, 2022 at: https://plus.lexis.com/document?crid=648749bc-a883-4dc1-bdb0-a0c93e44689f&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5C67-KTK1-F1WF-M0JD-00000-00&pdsourcegroupingtype=&pdcontentcomponentid=500749&pdmfid=1530671&pdisurlapi=true

U.S. Attorney's Office (Monday, March 27, 2023). *Brooklyn Man Pleads Guilty and Is Sentenced for Hacking into Online Accounts of Wegmans Customers*. Press Release of U.S. Attorney's Office, Western District of New York. Link: https://www.justice.gov/usao-wdny/pr/brooklyn-man-pleads-guilty-and-sentenced-hacking-online-accounts-wegmans-customers

U.S. Department of Justice (February 10, 2017). *Leader of three worldwide cyberattacks sentenced to 8 years for computer intrusion and access device fraud conspiracies*. Link: https://www.justice.gov/

usao-edny/pr/leader-three-worldwide-cyberattacks-sentenced-8-years-computer-intrusion-and-access#:~:text=Earlier%20today%2C%20at%20the%20federal,financial%20system%20between%202011%20and

U.S. Department of Justice (February 16, 2017). *Florida man sentences for hacking, spamming scheme that used stolen email accounts.* Link: https://www.justice.gov/opa/pr/florida-man-sentenced-hacking-spamming-scheme-used-stolen-email-accounts#:~:text=Timothy%20Livingston%2C%2031%2C%20of%20Boca,U.S.%20District%20Judge%20William%20J

Xie, Yan and Mujtaba, B. G. (2008). Strategies for Information Systems candidates and job seekers in the twenty-first century workplace. *Review of Business Information Systems Journal,* 12(1), 7-15.

Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. Link: https://h2o.law.harvard.edu/text_blocks/5660 ; https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Wee-Ellis, O., Dorsett, A., Montfort, C., Valdes, N. and Mujtaba, B. G. (2014). Communicating as a Woman in the Information Technology (IT) World. *International Journal of Gender and Women's Studies*, 2(2), 61-74. Link: http://ijgws.com/vol-2-no-2-june-2014-abstract-3-ijgws

Wilkinson, T. and Reinhardt, R. (2015). Technology in Counselor Education: HIPAA and HITECH as Best Practice. *Professional Counselor, 5*(3), 407-418.

Wozniak, Steve (February 9, 2023). Apple co-founder Steve Wozniak discusses AI race between Google and Microsoft. *CNBC Squawk Box*. Link: https://www.cnbc.com/video/2023/02/09/apple-co-founder-steve-wozniak-discusses-ai-race-between-google-and-microsoft.html