Effects of Technology on Cybercrimes on Business and Social Media

Joshua Nagathota[1], Jothsna Kethar[#] and Sarada Prasad Gochhayat, Ph.D.[#]

[1]Central Bucks High School South
[#]Advisor

ABSTRACT

In today's world, technology has become an ever-growing factor in our lives and ever since COVID-19, we have seen the rise of a digital, AI, world. Technology has greatly developed, evolved, and impacted the world since 2020. It has made lives more accessible in terms of communication and interactions. Instead of commuting to work every day, many businesses turned to ZOOM or TEAMS calls. Instead of having a meet-up with friends, you could Facetime. The world was forced to move online leaving the real world behind. However, many people overlook technology's impact on today's world. Cybercrime and cyber attacks are some of the many problems that continue to arise. With the sudden move to the online world, cybersecurity was a term many people hadn't grasped yet, leading many people to not understand the risk of not protecting their data online. Advancing technology has made many cybercrimes more common because people have personal information online linking bank accounts, addresses, and phone numbers left unprotected. Different cyber-attacks include malware and ransomware attacks, identity theft and fraud, phishing and spear phishing, cyber espionage, cyber extortion, crypto jacking, etc. The sectors that have been most affected are business and social media with Identity theft, spear-phishing, and fraud as leading attacks. The leading cybercrimes for these sectors are identity theft and ransomware attacks. For future generations, people have to learn about cyber-security and cybercrimes. This paper explains what cybercrime and cyber-attacks are, with how and why they happen. It will also explain technology's impact on cybercrimes and ways to prevent and protect future businesses and devices from potential cyber threats.

Introduction

In this past decade, technology has drastically changed from phones to laptops to computers, and eventually to the invention of the Internet. With the advancements in technology cybercrime, and cyber attacks have become more frequent in today's world. As a result of the COVID-19 pandemic, there has been a 600% increase in cybercrime, which involves anything from theft, embezzlement, data hacking, and data breaches (Mclean, 2023). The quarantine affected all levels of business, as they were forced to take their work into the digital world. The pandemic made cybercrime more recurrent because of the uncertainty surrounding remote work and how to secure your company against these unknown threats (Mclean, 2023). In 2020, Cyber attacks were ranked the fifth greatest risk and have since spread throughout the public and private sectors (Mclean, 2023). This dangerous industry is expected to keep expanding in 2023 as the number of IoT (Internet of things (IoT) refers to a network of physical objects connected to the internet that contain sensors, and software that allow for data sharing (Oracle, 2023)) cyberattacks is predicted to double by 2025 (Mclean, 2023). Experts say that cybercrime by itself will cost worldwide companies an estimated $10.5 trillion by 2025 (Mclean, 2023). The US lost about $4 Billion from cyberattacks in 2020; caused by technology flaws and users' inadequate security awareness cybercriminals were presented with opportunities for low-risk, high-reward gain (United States Department of State, 2023). With a population of almost 12 million, Pennsylvania ranks top 10 in the number of internet crimes during 2021-2022 (Susan, 2022). Pennsylvania also ranks in the top 5 for victim loss, as the total loss for Pennsylvania victims was $207 million (Susan, 2022). Cybercrime has become a big

predicament in today's world as we move closer to AI and the online world. And technology has had a role in making the attacks more common, as these attacks are becoming easier to gain access to and use. Although technology's evolution has also given us different types of cyberattacks, it has also given us ways to protect and prevent ourselves from these attacks.

What is Cybersecurity?

To talk about cybercrimes, people must first get familiar with the concept of cybersecurity. Cybersecurity refers to the practice of protecting networks, devices, programs, and data from attacks or unauthorized access (De Groot, 2023). It is also the practice of promising confidentiality, integrity, and availability of information (CISA.gov, 2021). There are many different elements of cybersecurity that an organization needs to ensure its information system (De Groot, 2023). Here are five important elements. Network security is the act of protecting networks against unauthorized users, access, and attacks (De Groot, 2023). Constant updates of apps and testing of programs are labeled as application security (De Groot, 2023). Protecting remote access to a company's network is referred to as Endpoint security (De Groot, 2023). Data security and identity management are similar in the fact that both require understanding and protection of the company's and customer's information (De Groot, 2023). Cybersecurity is of utmost importance for major organizations like the government and healthcare companies. A critical portion of data, personal, and financial, is stored on computers (De Groot, 2023). As these organizations transmit data across different networks, protection of said data is vital, as leaks and exposures could have drastic consequences (De Groot, 2023). As cyber-attacks increase in sophistication, steps must be taken to ensure sensitive data doesn't get out (De Groot, 2023).

Understanding Cybercrime

Cybercrime has been a big part of the world economy, costing many businesses millions in damages and lost data and personal information. The first recorded cyber-attack happened before the internet was created in France (Wolf, 2023). In 1834, attackers stole financial market information by accessing the French telegraph system (Wolf, 2022). Since then cybercrime has grown exponentially marked by the intriguing evolution of tactics and techniques used (Wolf, 2022). Spurred on by the digital revolution, cybercriminals were early adopters of technology, using their intelligence to engineer cunning ways to attack people and organizations (Wolf, 2022). Cybercrime is defined as criminal activity that either targets a computer, a computer's network, or a networked device (Kaspersky, 2023). Cybercrime is committed by skilled hackers or cybercriminals who want profit, but on occasion, cybercrime aims to damage computers and networks for political or personal reasons (Kaspersky, 2023). It can be carried out by individuals or groups with relatively little technical skill, or by highly organized global criminal groups (Brush, 2021).

As shown in Figure 1, cyber-attacks increased by nearly 6% from 80 to 86 in one year from 2020-2021. During the pandemic criminals took advantage of networks and businesses as they moved to digital work environments, Malware attacks were at an all-time high increasing 358% from 2019 (Griffiths, 2023). In 2022 alone, over $8 billion was lost as a result of cybercrime, this number will only increase in the coming years (Flynn, 2023). Cybercrime has become so common that nearly 1 in 4 Americans have fallen victim to a cyberattack (Flynn, 2023). And over 50% of organizations have been hit by professional hackers that can now infiltrate their systems in under 12 hours (Flynn, 2023). Data breaches have also been a major issue for many businesses across the US. Costing on average $4 to $9 million per data breach and keep in mind there are thousands of successful breaches every year (Flynn, 2023). There are more examples of cybercrime like identity theft, financial theft, ransomware, malware attacks, phishing and spear phishing, data loss and damage, etc. (Kaspersky, 2023).

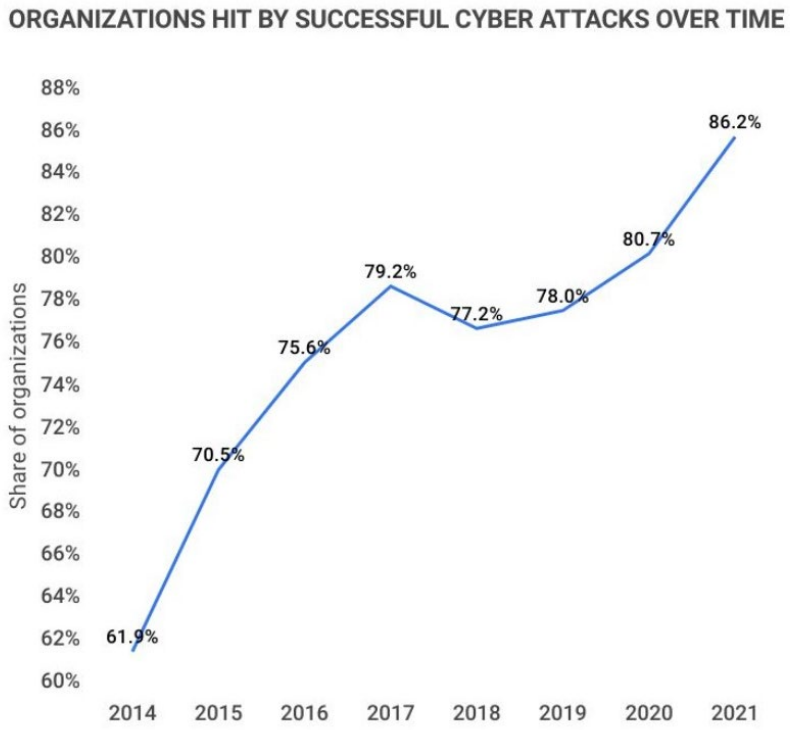

Figure 1. The image shows the gradual increase of successful cyberattacks from the year 2014. Adapted from "30+ CONCERNING CYBERCRIME STATISTICS [2023]: THE COST, TRENDS + FACTS," by J. Flynn, 2023.

As shown in Figure 1, cyber-attacks increased by nearly 6% from 80 to 86 in one year from 2020-2021. During the pandemic criminals took advantage of networks and businesses as they moved to digital work environments, Malware attacks were at an all-time high increasing 358% from 2019 (Griffiths, 2023). In 2022 alone, over $8 billion was lost as a result of cybercrime, this number will only increase in the coming years (Flynn, 2023). Cybercrime has become so common that nearly 1 in 4 Americans have fallen victim to a cyberattack (Flynn, 2023). And over 50% of organizations have been hit by professional hackers that can now infiltrate their systems in under 12 hours (Flynn, 2023). Data breaches have also been a major issue for many businesses across the US. Costing on average $4 to $9 million per data breach and keep in mind there are thousands of successful breaches every year (Flynn, 2023). There are more examples of cybercrime like identity theft, financial theft, ransomware, malware attacks, phishing and spear phishing, data loss and damage, etc. (Kaspersky, 2023).

Cyber Attacks

A cyber-attack is essentially an attempt to comprise a device, network, or computer (Equifax, 2023). Data, opportunity, and motive are all that are required for a cyber-attack to begin (Brush, 2021). While images of intricate teams of computer experts with high-tech equipment, typing away lines of code, are what people think of when they hear terminology like "cyber-attacks" and "hackers" the reality is quite different (Equifax, 2023). Cyber-attacks are much more likely to occur through everyday mistakes like a user selecting an easy-to-guess password or failing to change the default password on something like a router (Equifax, 2023). Looking for new strategies to accomplish their objectives without being discovered and arrested many cybercriminals carry out their attacks using a variety of threat vectors (Brush, 2021). The most common spots for these attacks to happen are the government and businesses, leading

to millions in damages and data loss (Equifax, 2023). There are many motives behind cyber-attacks. Politically motivated cyber-attacks may have more harmful intent, such as leaking sensitive intelligence, private communications, and data (Equifax, 2023). Cyber-attacks may also go further; for instance, government-backed hackers could create software to destroy a weapons program or other infrastructure (Equifax, 2023). Cyber-attacks can also result in data breaches, where large amounts of information are leaked online and then used by criminals to commit fraud (Equifax, 2023). Data such as credit card numbers, names, and addresses can be all some cybercriminals need to carry out identity theft (Equifax, 2023).

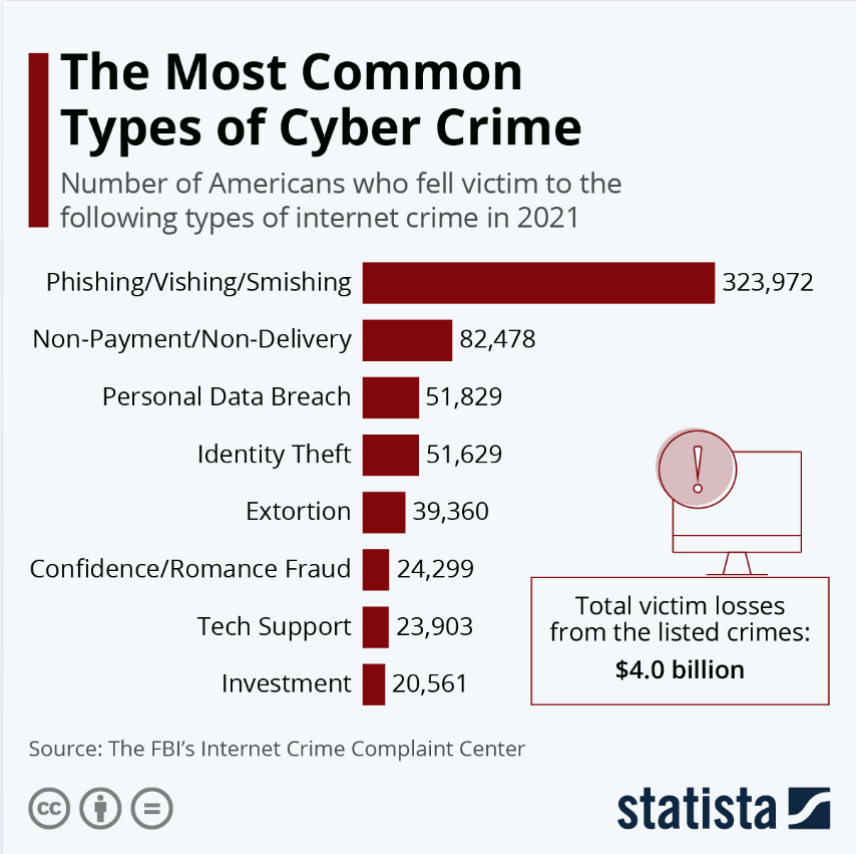

Figure 2. This model was produced by "The FBI's Internet Crime Complaint Center" in 2021. It shows the most common types of cybercrimes and the number of victims. Adapted from "Statista," by F. Richter, 2022.

As shown in Figure 2 phishing had the most victims in 2021 and those have risen since then. Phishing is when spam emails, messages, and calls are sent with the intention of tricking the recipient. These messages usually contain links or infected attachments that ask for confidential information, and when entered the sender can gain access to that information. (Kaspersky, 2023). Phishing still is the most common type of attack as 3 billion spam emails are sent daily (Griffiths, 2023). There are other various ways cybercriminals aim to get paid, such as attacks like cyber extortion, crypto-jacking, and cyber espionage (Brush, 2021).

Effects of Cybercrimes on Businesses

The ever-evolving digital world affects cybersecurity in many ways people don't realize (Harrington, 2020). Digital technology has given many benefits, comforts, and conveniences that couldn't even be imagined decades ago (Wellisz,

2016). The internet makes everything easier to access. Students and scholars can complete research in hours rather than spend those hours in libraries searching for books (Wellisz, 2016). The rates of cybercrime have been consistently growing with the rate of developing technology (Harrington, 2020). As more businesses transition to remote work schedules as a result of the pandemic, cybercriminals may target the personal information of individual or corporate data for theft and resale, making backup data protection even more crucial (Brush, 2021). This connected world offers more opportunities for cybercriminals to gain access to personal information that can turn into fraud (Wellisz, 2016). Here are some examples of how technology has impacted cybercrime in businesses.

There have been countless cyberattacks on businesses worldwide, but it was found that small and medium businesses were the most targeted by cybercrimes (Mclean, 2023). 43% of cyber-attacks are aimed toward them, but only a small percentage can defend themselves (Mclean, 2023). These attacks drastically alter a small business, affecting the business employees, money, and infrastructure (Flynn, 2023). It's important to remember that these businesses were just launched meaning they don't have enough funding yet to set up security measures (Mclean, 2023). Damages to their systems may lead to fines for loss of sensitive data, causing debt (Brush, 2021). Researchers found that almost 60% of SMBs close after a cyber-attack (Flynn, 2023).

Being a larger company in today's world means that you are always on hacker's watchlists. They are always on the lookout for potential employees in these companies to exploit through social engineering and scams (Allinson, 2022). With advancing technologies skilled hackers are finding holes and loopholes and gaps in corporate security systems easier (Harrington, 2020). This then allows them to gain access to the employees' personal information and even the companies' secure files and data, which is a major cybersecurity threat (Harrington, 2020). Targeting employees may also be known as spear phishing (Harrington, 2020). Unlike regular phishing targeting random people, spear phishing is mainly for business secrets, fraud, money, and momentary gain (Allinson, 2022). With technological advancements, hackers are now able to pose as employees and send emails to others containing malicious links to steal information. (Allinson, 2022).

Another part of technology's impact on cybercrime is how everything is more digital. Even though most digital data is usually backed up and stored behind passwords, it's still on a shared network which is at risk for hacks (Harrington, 2020). Data stored on shared networks runs the risk of being hacked and hackers gaining access to the network and personal data putting businesses and individuals at a disadvantage (Allinson, 2022). Additionally, as businesses move to cloud computing and save documents on the cloud, they are also at risk of cybersecurity threats (Allinson, 2022). Ransomware attacks becoming more prevalent in businesses is a major concern. Ransomware attacks happen when hackers gain access to an organization's systems and encrypt any valuable data until a ransom is paid. Over half of US organizations have had their data successfully encrypted in ransomware attacks, costing over $2 million per attack (Griffiths, 2023). Attack frequency has also multiplied from 2020-2022 from 40 to less than 10 seconds. Therefore, with advancing technology extreme caution must be taken and safeguards be in place to protect the data in the cloud (Harrington, 2020).

Effect of Cybercrime on Social Media

The internet's development has led to many different inventions and ideas but the most important is social media (Riley, 2021). We can't deny the impact social media has already had on today's generation's lives and businesses (Smitherson, 2012). The rise of social media has led to many different ways of communication and sharing (Smitherson, 2012). Apps like Snapchat, Instagram, Facebook, and Twitter have all shown us revolutionary ways to use the internet for public and private purposes (Smitherson, 2012). iPhones and computers make everyday lives more manageable, if you forget something or are lost you can use your phone and get your answers (Wellisz, 2016). However, many people worry about privacy and their digital footprint. They worry about how a potential leak of data like calls and messages can leave a digital trail that can be exposed by hackers (Wellisz, 2016). As we move into the future these networks will rapidly change the way we communicate and interact internationally (Riley, 2021). It was found that around 4.8 billion or 60% of the world have one or more of the major social media platforms (Chin, 2023).

However, the rising number of cybercrime cases reported every year is in accordance with the emergence of social media (Riley, 2021). Because everyone's data was left unprotected, it made many hackers' jobs effortless. While these platforms have made communications, and interactions easier for many, they also expand people's and businesses' exposure to many cyber threats in the following ways (Chin, 2023).

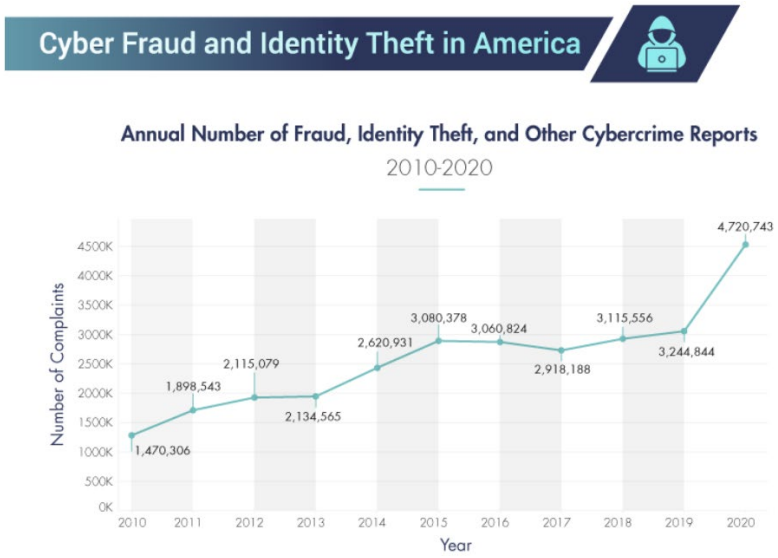

Figure 3. This model was produced by "Consumer Sentinel Network Annual Reports, 2010 and 2020." This image shows the increase in the annual number of frauds, and identity theft from 2010-2020. Adapted from "Beyond Identity" 2021.

Identity fraud is defined as when cybercriminals buy or sell identity information on darknet markets, allowing others to use it to access their valuable accounts, cards, and health information (Brush, 2021). Identity theft is the key threat to many social media users (Smitherson, 2012). Billions of online users use most of their personal information in order to get registered with one or more social media platforms (Smitherson, 2012). Cybercriminals engage in social media to gain access to codes and passwords (Allinson, 2022). Experienced hackers can easily gain access to users' accounts and use the information to go into bank accounts (Harrington, 2020). The average social media user usually shares most if not all their data including name, age, location, family members, birthday, and even phone numbers, and addresses (Harrington, 2020). A significant number of media users are ignorant about what and how much information they enter into their accounts (Riley, 2021). They don't think about how the info they enter can be relevant to the cybercriminals (Riley, 2021). And most platforms do not care or take into account the security of their user's details, so the info is left susceptible to hacks (Riley, 2021). This is the main reason many cybercriminals choose their targets and aim to hack these accounts (Smitherson, 2012). Even if you don't share this information, hackers will still try to gain access to your accounts on other platforms and steal your identity (Allinson, 2022). Identity theft from social media then converts into phishing as criminals can sell identities to other criminals to use to commit illegal activities and be concealed from law enforcement (Riley, 2021). With more than 45% of cell phone users having smartphones, there is a greater risk because most of those users keep their data stored in the device (Harrington, 2020). With advancing mobile technology, there are increasing opportunities for cybercriminals to gain access to the devices' information (Allinson, 2022).

Apart from hackers having access to your information, most sites and social media apps ask for a location (Harrington, 2020). The evolution of social media has given users the ability to update their "status (Riley, 2021). Certain social media users on apps like Snapchat and Instagram often post stories with their locations in places like restaurants, schools, and homes (Allinson, 2022). That means cybercriminals on social media can see where you go

and where you are not. (Harrington, 2020). Some platforms also keep spots to show relationships with friends and families, meaning the hackers will also try to track them (Riley, 2021). Many modern social media apps allow users to post photos, and videos to update their "status" and locations, allowing cybercriminals to pin locations and track their targets (Riley, 2021). If the user pins their locations, relationships, and photos, it makes it easier to track them and opens up more threats to other family members or friends (Riley, 2021). Some people even go as far as providing information about their credit or debit cards to purchase items through social media apps (Smitherson, 2012). A form of financial theft includes credit card fraud. Stolen payment cards can be bought and sold in bulk on darknet markets, where hacking groups that have stolen mass quantities of credit cards profit by selling to lower-level cybercriminals who profit through credit card fraud against individual accounts. An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers (Brush, 2021).

Ways to Prevent Cyber Attacks Going into the Future

As we go into a more digital future, cyber-attacks are going to become more recurrent. Future generations will have to conform to a society with these attacks and learn how to prevent them. Fortunately for us as technology has advanced, so has the ability to detect potential threats and attacks before they happen (Harrington, 2020). There are many different ways to protect against these attacks. Training your staff on cyber-attack prevention and educating them on current cyber-attacks is one of the most effective ways to protect against cyber-attacks and all types of data breaches (Leaf, 2022). Employee awareness is crucial because one of the most common ways cybercriminals access your data is through your employees (Leaf, 2022). They will send phony emails pretending to be someone from your company, asking for personal information or access to certain files. Links often look legitimate to an untrained eye and it's easy to fall into the trap (Leaf, 2022). Things to check for are suspicious links in emails, messages, and calls. It is important to remember not to open any suspicious links and attachments in emails sent to you (Kaspersky, 2023). Also, make sure to have a secure Wi-Fi connection or use a trustable VPN when accessing personal information. That's why companies have to create a workplace that recognizes the importance of cybersecurity (Turio, 2023). Reports say that 70% of hackers target small businesses because their websites don't have many security measures (Turio, 2023). It's vital to explain ways to prevent cyberattacks and to have a response plan ready in case of an attack (Turio, 2023).

Vulnerabilities are frequently found in all software, and once they are, malicious individuals work quickly to exploit them in order to attack computers and networks (Leaf, 2022). Vulnerabilities can affect any device that runs software (Emily, 2022). Software written and distributed with malicious intent, such as viruses, worms, and spyware, can infect a device by downloading programs and files from the internet (Emily, 2022). Sources like email attachments, app downloads, and unauthorized software installations can infect your device with malware (Emily, 2022). After this happens you will suffer from data loss, malfunctioning systems, and infections (Emily, 2022). It is a good idea to invest in patch management software that keeps your system up to date with updates (Leaf, 2022). Software that is licensed and supported will protect your device from potential attacks (Emily, 2022). An anti-virus software is something to invest in also. Its purpose is to scan your device to detect and remove any viruses, protecting it from any future problems (Kaspersky, 2023).

Firewalls are also an efficient way to prevent cyberattacks. By using firewalls and data flow policies you can restrict access to certain services and reduce your device's exposure to attacks (Emily, 2022). Every device that accesses your network should be protected by a firewall, which can limit network traffic and defend against cyber-attacks by blocking traffic under a predetermined set of rules (Emily, 2022). Before they can cause any harm, a firewall system will stop any brute-force attacks made against your network and/or systems (Leaf, 2022). Putting your networks behind a firewall is the most effective to protect yourself from most cyberattacks (Leaf, 2022).

Another way to effectively protect your device is with passwords. So much of your private life is hidden behind passwords, including private conversations, bank accounts, etc. (Stouffer, 2023). But many could care less about the strength of the password they set for important sites. Because of this, hackers will focus their efforts on hacking and stealing your passwords in order to access your files, and money (Stouffer, 2023). To reduce these risks,

we can prioritize our passwords (Stouffer, 2023). In 2022, more than 24 million passwords were stolen (Digital Shadows, 2022). And 80% of data breaches relate back to weak or overused passwords (LastPass, 2021). The best way to counteract this is to create better, stronger passwords without having to reuse them for different sites. Changing passwords often will maintain a high level of protection against external and internal threats (Leaf, 2022).

Conclusion

Technology has greatly impacted our daily lives, especially in today's world. The evolution of the internet and its role in social media and businesses have really affected people's lives. The AI and digital world have taken over our once-physical lives. COVID-19 forced the world into the online world, not knowing what the downsides could be and the potential risks people faced by storing all their personal information online. The world has seen a sharp increase in the rate of cybercrimes being committed. This paper defines cybercrime as criminal activity in which the user targets a computer and or a computer's network. Identity theft, financial fraud, ransomware, malware attacks, and data breaches are some examples. It also explains the impact cyber-attacks have had on business and social media sectors. The main drives for cyberattacks are for money, momentary gain, or political agenda. And they usually happen to people who have weak passwords and protection and have most of their information online. That's why it is crucial the future generation learn about cybersecurity and how to prevent these attacks. Some of the ways we can do that are by implementing firewalls, having strong passwords, updating software, and teaching employees about prevention and protection. So, by teaching future generations about cybersecurity we can start lowering the rate at which cybercrimes happen. With technology evolving, we can soon eradicate cybercrime altogether.

Acknowledgments

I would like to thank Professor Sarada for taking the time to teach me about the basics of cybersecurity and getting me into the topic more. Also, I would like to thank Prof. Virgel for all the tips and advice on how to make this research paper better and Coach Jo for helping me write my first research paper.

References

10 ways to prevent Cyber attacks - Leaf. (2022). Leaf. https://leaf-it.com/10-ways-prevent-cyber-attacks/

139 password statistics to help you stay safe in 2023 - Norton. (n.d.). https://us.norton.com/blog/privacy/password-statistics#:~:text=And%20because%20passwords%20are%20so,(Digital%20Shadows%2C%202022)

Allinson, M. (2022). *How does cyber technology affect security?* Robotics & Automation News. https://roboticsandautomationnews.com/2022/12/07/how-does-cyber-technology-affect-security/58479/#:~:text=As%20technology%20advances%2C%20so%20do,poses%20a%20critical%20cybersecurity%20threat

Brush, K., Rosencrance, L., & Cobb, M. (2021). cybercrime. *Security*. https://www.techtarget.com/searchsecurity/definition/cybercrime?Offer=abt_pubpro_AI-Insider

Cybercrime - United States Department of State. (2023). United States Department of State. https://www.state.gov/cybercrime#:~:text=In%202020%20alone%2C%20the%20FBI,them%20offline%20during%20the%20pandemic.

Cybercrimemag. (2021). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,$3%20trillion%20USD%20in%202015.

Emily. (2022). Cybercrime is on the rise, Is your business prepared? *Open Access Government*. https://www.openaccessgovernment.org/cybercrime-is-on-the-rise-is-your-business-prepared/143070/#:~:text=Un%2Dtargeted%20cyber%2Dattacks%20such,21%20(Source:%20ActionFraud).

Flynn, J. (2023). 30+ Concerning Cybercrime Statistics [2023]: The Cost, Trends + Facts. *Zippia*. https://www.zippia.com/advice/cybercrime-statistics/

Griffiths. (2023). The Latest Cyber Crime Statistics (updated August 2023) | AAG IT Support. *AAG IT Services*. https://aag-it.com/the-latest-cyber-crime-statistics/

Harrington, J. (2023). Ten ways evolving technology affects cybersecurity. *Utica University*. https://programs.online.utica.edu/resources/article/ten-ways-evolving-technology-affects-cybersecurity

How cyber attacks happen | Equifax UK. (n.d.). https://www.equifax.co.uk/resources/identity-protection/how-cyber-attacks-happen.html

Mclean, M. (2023). 2023 Must-Know Cyber Attack Statistics and Trends | Embroker. *Embroker*. https://www.embroker.com/blog/cyber-attack-statistics/#:~:text=Cybercrime%2C%20which%20includes%20everything%20from,security%20in%202023%20and%20beyond?

Richter, F. (2022). The Most Common Types of Cyber Crime. *Statista Daily Data*. https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/

Riley, B. (2021). *Effects of Social Media on Cybercrime - Criminal Law Essays*. LawAspect.com. https://lawaspect.com/effects-of-social-media-on-cybercrime/

Security Magazine. (n.d.). https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

Smitherson, D. (2012). *Impact of Cyber Crime and Security on Social Media*. Social Media Today. https://www.socialmediatoday.com/content/impact-cyber-crime-and-security-social-media

The Dark Side of Technology -- Finance & Development, September 2016. (2016). https://www.imf.org/external/pubs/ft/fandd/2016/09/wellisz.htm#:~:text=A%20connected%20world%20offers%20new,return%20for%20a%20decryption%20key.

The Impact of Social Media on Cybersecurity | UpGuard. (n.d.). https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity

Turio. (2023). Top Ways to Prevent Cyber Security Threats. *CiS*. https://www.cisin.com/coffee-break/technology/top-ways-to-prevent-cyber-security-threats.html

What is Cyber Security? Definition, Best Practices & Examples. (n.d.). Digital Guardian. https://www.digitalguardian.com/blog/what-cyber-security

What is cybercrime? How to protect yourself from cybercrime. (2023). usa.kaspersky.com. https://usa.kaspersky.com/resource-center/threats/what-is-cybercrime

What is Cybersecurity? | CISA. (2021). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/what-cybersecurity

What is the Internet of Things (IoT)? (n.d.). https://www.oracle.com/internet-of-things/what-is-iot/

What States Have The Most Cybercrime? (n.d.). https://www.b2z-insurance.com/blog/top-ten-states-with-the-most-cybercrime#:~:text=Pennsylvania%20ranked%208th%20out%20of%2050%20for,a%20population%20of%20about%2011.78%20million%20people%2C

Wolf, A. (2023). A brief history of cybercrime. *Arctic Wolf*. https://arcticwolf.com/resources/blog/decade-of-cybercrime/#:~:text=Still%2C%20cybercrime%20didn't%20really,from%20their%20data%20and%20dollars.