International Journal of Research in Engineering, Science and Management
Volume 5, Issue 4, April 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

Need for Cyber Security Tools and Knowledge

Drishan Dutt[1*], Sanidhya Pandey[2], Sankalp Arora[3], Manasvi Tripathi[4], Konark Kumar Gupta[5]
[1,2,3,4,5]*B.Tech. Student, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India*

Abstract*: Beginning around 2013 there are 3,809,448 records taken from breaches consistently. 158,727 every hour, 2,645 every moment and 44 the entire day reports Cybersecurity Ventures. Cybersecurity is currently a worldwide need as cybercrime and computerized dangers fill in recurrence and intricacy. In any case, one of the significant obstructions to forestalling cybercrime is the cybersecurity labor force deficiency and absence of new experts piping into this industry. As per the Cybersecurity Jobs Report, there will be roughly 3.5 million unfilled cybersecurity occupations by 2021, while simultaneously episodes of worldwide cybercrimes are supposed to move to 6 trillions during that very year. No faltering that the tool of Cybersecurity makes our work exceptionally simple by guaranteeing the attainable quality of the capitals restricted in any organization. A business or society could look a gigantic harm if they are not genuine with regards to the security of their on the web event. In the present connected world, everybody helps from moderate cyber safeguard plans. At a separate level, a cybersecurity flare-up can result in aggregate from singularity robbery, to blackmail endeavours, to the harm of fundamental information similar family photos, etc. Researchers believe that everyone who has access to a laptop and a network connection, needs to have at least basic information about cyber threats. Cyber threats are those kinds of threats that have the potential to steal utmost important data without us even being aware of it. Malware whom we allowed to infiltrate in our system, can stay there for years and execute themselves whenever the attacker wishes to steal our data or to use our system to do something malicious to someone else in order to get a smooth evasion.

***Keywords*: Cybercrime, History, Effect of cyber-crime in personal life, Safeguide.**

1. Introduction

The aim of this study is to generate an understanding and awareness about the importance of cyber security in business, personal as well as corporate life. With the internet being the global platform that connects every bit of information and communication from one point to another. It is very important for individuals to educate themselves about the ways that hackers can steal our data. Throughout this paper readers will get basic as well as advanced knowledge of various cyber-crimes, intentions of cybercriminals, cyberwarfare theory with historic examples and most of the required knowledge for defending ourselves from cyber-attacks that happen on regular basis.

2. What is cyber-crime?

Cybercrime, additionally called computer crime, the utilization of a PC as an instrument to additional illegal finishes, for example, carrying out extortion, dealing with child porn and licensed innovation, stealing personalities, or abusing security. Cybercrime, particularly through the Internet, has filled in significance as the PC has become fundamental to business, diversion, and government.

In light of the early and broad reception of PCs and the Internet in the United States, the greater part of the earliest casualties and antiheroes of cybercrime were Americans. By the 21st 100 years, however, barely a villa remained anyplace on the planet that had not been moved by cybercrime of some sort.

New innovations set out new crook open doors yet scarcely any new sorts of crime. What recognizes cybercrime from customary crime? Clearly, one contrast is the utilization of the computerized PC, yet technology alone is lacking for any differentiation that could exist between various domains of crime. Crooks needn't bother with a PC to submit extortion, traffic in kid erotic entertainment and protected innovation, steal a character, or abuse somebody's security. That large number of exercises existed before the "cyber" prefix became universal. Cybercrime, particularly including the Internet, addresses an expansion of existing criminal way of behaving close by a few novel illegal exercises.

Most cybercrime is an assault on data about people, companies, or state-run administrations. Albeit the assaults don't happen on an actual body, they really do occur on the individual or corporate virtual body, which is the arrangement of educational properties that characterize individuals and organizations on the Internet. At the end of the day, in the advanced age our virtual personalities are fundamental components of day-to-day existence: we are a heap of numbers and identifiers in various PC information bases possessed by legislatures and enterprises. Cybercrime features the centrality of arranged PCs in our lives, as well as the delicacy of such apparently strong realities as individual personality.

A significant part of cybercrime is its nonlocal character: activities can happen in locales isolated by immense distances. This postures serious issues for policing already neighborhood or even public crimes currently require global collaboration. For instance, assuming an individual gets to youngster sexual entertainment situated on a PC in a country that doesn't boycott kid porn, is that individual carrying out a crime in a country where such materials are illegal? Where precisely does cybercrime occur? Cyberspace is basically a more extravagant rendition of the space where a telephone discussion happens,

*Corresponding author: drishandutt9@gmail.com

somewhere close to the two individuals having the discussion. As a planet-spreading over network, the Internet offers lawbreakers various concealing spots in reality as well as in the actual organization. Notwithstanding, similarly as people strolling on the ground leave denotes that a talented tracker can follow, cybercriminals leave hints with respect to their personality and location, regardless of their earnest attempts to cover their tracks. To follow such signs across public limits, however, worldwide cybercrime arrangements should be sanctioned.

3. Brief History

Cybercrime at first started with developers endeavoring to break into PC organizations. Some did it just for the fervor of getting to unquestionable level security organizations, yet others hoped to procure delicate, organized material. At last, culprits started to spoil PC structures with PC infections, which provoked breakdowns on private and business PCs.

PC infections are sorts of code or malware programs that can copy themselves and mischief or demolish data and systems. Exactly when PC infections are used for a tremendous extension, likewise with bank, government or clinical facility organizations, these exercises may be requested as cyberterrorism. PC software engineers also participate in phishing stunts, for example, mentioning monetary equilibrium numbers, and Mastercard burglary. Underneath referred to are a part of the eminent digital attacks since before time began.

1834 — French Telegraph System — A couple of hoodlums hack the French Telegraph System and take monetary market data, actually leading the world's first cyberattack.

1870 — Switchboard Hack — A youngster recruited as a switchboard administrator can disengage and divert calls and utilize the line for individual use.

1878 — Early Telephone Calls — Two years after Alexander Graham Bell imagines the phone, the Bell Telephone Company dismisses a gathering of high school young men from the phone framework in New York for over and over and purposefully misleading and detaching client calls.

1903 — Wireless Telegraphy — During John Ambrose Fleming's most memorable public exhibit of Marconi's "secure" remote telecommunication innovation, Nevil Maskelyne disturbs it by sending offending Morse code messages undermining the development.

1939 — Military Codebreaking — Alan Turing and Gordon Welchman foster BOMBE, an electro-mechanical machine, during WWII while functioning as codebreakers at Bletchley Park. It assists with breaking the German Enigma codes.

1940 — First Ethical Hacker — Rene Carmille, an individual from the Resistance in Nazi-involved France and a punch-card PC master who possesses the machines that the Vichy administration of France uses to deal with data, figures out that the Nazis are utilizing punch-card machines to process and find Jews, volunteers to allow them to utilize his, and afterward hacks them to ruin their arrangement.

1955 — Phone Hacker — David Condon whistles his "Davy Crockett Cat" and "Canary Bird Call Flute" into his telephone, testing a hypothesis on how telephone frameworks work. The framework perceives the mystery code, accepts he is a worker, and interfaces him to a significant distance administrator. She interfaces him to any telephone number he demands for nothing.

1957 — Joybubbles — Joe Engressia (Joybubbles), a visually impaired, 7-year-old kid with amazing pitch, hears a piercing tone on a telephone line and starts whistling along to it at a recurrence of 2600Hz, empowering him to speak with telephone lines and become the U.S's. first telephone programmer or "telephone phreak."

1962 — Allan Scherr — MIT sets up the principal PC passwords, for understudy security and time limits. Understudy Allan Scherr makes a punch card to fool the PC into printing off all passwords and utilizations them to sign in as others after his time expires. He likewise shares passwords with his companions, prompting the primary PC "savage." They hack into their instructor's record and leave messages ridiculing him.

1969 — RABBITS Virus — A mysterious individual introduces a program on a PC at the University of Washington Computer Center. The subtle program makes duplicates of itself (reproducing like a hare) until the PC over-burdens and quits working. Being the primary PC virus is thought.

1970-1995 — Kevin Mitnick — Beginning in 1970, Kevin Mitnick enters the absolute most profoundly protected networks on the planet, including Nokia and Motorola, utilizing elaborate social designing plans, fooling insiders into giving over codes and passwords, and utilizing the codes to get to inner PC frameworks. He turns into the most-needed cybercriminal of the time.

2005 — Phone Busters — Phone Busters reports 11K+ wholesale fraud grievances in Canada, and absolute misfortunes of $8.5M, making this the quickest developing type of purchaser misrepresentation in North America.

2005 — Polo Ralph Lauren/HSBC - HSBC Bank sends letters to in excess of 180,000 Mastercard clients, cautioning that their card data might have been taken during a security break at a U.S. retailer (Polo Ralph Lauren). A DSW information break likewise uncovered exchange data from 1.4 million Mastercards.

2017 — WannaCry — WannaCry, the main known illustration of ransomware working through a worm (viral programming that reproduces and circulates itself), focuses on a weakness in more seasoned adaptations of Windows OS. In no time, a huge number of organizations and associations across 150 nations are kept out of their own frameworks by WannaCry's encryption. The aggressors request $300 per PC to open the code.

2018 — Marriot International (Starwood) — Using taken accreditations, a danger entertainer had the option to break Marriott Hotels frameworks through a Remote Access Trojan (RAT). Information from north of 500 million visitors, including delicate information like Visa and identification data, was taken.

2018 — Dubsmash — The well-known video web based stage found 161.5 million client records were put available to be purchased on the dull web. Records included subtleties like name, email address, and scrambled passwords.

2019 — Alibaba — A selling worker secretly got 1.1 million bits of information including Alibaba client contact data and spilled it to a wholesaler's staff part during the November 11 Singles' Day shopping celebration.

2019 — Facebook — Information connecting with in excess of 530 million Facebook clients is uncovered by an obscure programmer including telephone numbers, account names, and Facebook IDs.

2020 — Sina Weibo — 538 million clients' data is taken from Sina Weibo, what could be compared to Twitter, and coursed on the dull web.

2020 — SolarWinds — FireEye, an unmistakable network safety firm, declared they were a casualty to a country state assault. The security group announced their Red Team toolbox, containing applications involved by moral programmers in entrance tests, was taken. FireEye found a store network assault while it was researching the country state assault on its own Red Team tool compartment. The specialists coincidentally found proof that assailants entered an indirect access in the SolarWinds programming "trojanizing" SolarWinds Orion business programming updates to disperse malware.

2021 — Colonial Pipeline — a ransomware assault constrained Colonial Pipeline, a U.S. energy organization to close down its whole fuel dissemination pipeline — and subsequently undermined gas and stream fuel conveyance across the U.S. east coast. Pioneer Pipeline paid almost $5 million to Eastern European programmers to assist with reestablishing the country's biggest fuel pipeline.

2021 — Accenture — The LockBit ransomware posse penetrated Accenture's organizations, encoded documents and requested $50 million to try not to have their scrambled records sold on the dim web.

4. Cyber Criminal’s Intentions

Cybercrime can take countless structures, going from the illegal offer of labor and products to taking on the appearance of someone else to steal cash from monetary organizations.

Data breach-One of the most well-known web-based dangers is a data breach. Data breaches can take many structures, however at its center, a data breach happens when a crook illegally gets to significant and frequently private data from an organization's database. These assaults are distressingly normal as in 2014 there were 783 data breaches in the United States alone. A few data breaches include the assortment of client's Mastercard data, while others include exclusive data well defined for the actual organization. Frequently these assaults lead to the crooks taking steps to deliver the impacted organizations' data except if they are paid off.

Selling illegal merchandise Beyond the danger of data breaches, cybercriminals additionally take part in the flourishing internet-based environment of trading an items and administrations, the majority of which have been considered illegal in nations all over the planet. One of the most notable centers of this type of cyber movement was Silk Road whose clients bought in excess of 213 million dollars in merchandise before the site was closed somewhere near the police. By far most of the webpage's contributions were illegal medications and at the time the website was closed down, there were in excess of 10,000 things recorded, around 7,000 of which were illegal medications like marijuana, MDMA and heroin.

Bitcoin and the dark Web-Silk Road worked essentially by utilization of an internet-based cash called Bitcoin, which permits both the buyer and the dealer to remain totally unknown. Through Bitcoin, the clients of Silk Road had the option to carry on their business throughout the span of quite a long while. In the end, nonetheless, government specialists had the option to find the organizer behind Silk Road, who has since been condemned to life in jail without the chance for further appeal for his job in working the website. While Silk Road itself has been closed down, an assortment of destinations has created to have its spot.

5. Types of Cyber Crime

Categories of Cybercrime:

There are three major categories that cybercrime falls into: individual, property and government. The types of methods used and difficulty levels vary depending on the category.

Property: This is like a genuine occasion of a crook illegally having a singular's bank or charge card subtleties. The programmer steals an individual's bank subtleties to get sufficiently close to reserves, make buys on the web or run phishing tricks to move individuals to offer their data. They could likewise utilize vindictive programming to get close enough to a web page with private data.

Individual: This class of cybercrime includes one individual dispersing pernicious or illegal data on the web. This can incorporate cyberstalking, circulating sexual entertainment and dealing.

Government: This is the most uncommon cybercrime, yet is the most genuine offense. A crime against the public authority is otherwise called cyber psychological oppression. Government cybercrime incorporates hacking government websites, military websites or dispersing misleading publicity. These lawbreakers are normally psychological militants or hostile legislatures of different countries.

DDoS Attacks: These are utilized to make a web-based assistance inaccessible and bring the network somewhere near overpowering the webpage with traffic from an assortment of sources. Enormous networks of contaminated gadgets known as Botnets are made by storing malware on clients' PCs. The programmer then hacks into the framework once the network is down.

Botnets: Botnets are networks from compromised PCs that are controlled remotely by far off programmers. The distant programmers then send spam or assault different PCs through these botnets. Botnets can likewise be utilized to go about as malware and perform pernicious undertakings.

Identity Theft: This cybercrime happens when a lawbreaker accesses a client's very own data to steal reserves, access classified data, or partake in expense or medical coverage extortion. They can likewise open a telephone/web account in your name, utilize your name to design a crime and guarantee government benefits in your name. They might do this by figuring out client's passwords through hacking, recovering

individual data from virtual entertainment, or sending phishing messages.

Cyberstalking: This sort of cybercrime includes online badgering where the client is exposed to a plenty of online messages and messages. Commonly cyberstalkers utilize web-based entertainment, websites and web indexes to scare a client and impart dread. Generally, the cyberstalker knows their casualty and causes the individual to feel apprehensive or worried for their wellbeing.

Social Engineering: Social designing includes lawbreakers connecting with you ordinarily by telephone or email. They need to acquire your certainty and generally act like a client assistance specialist so you'll give the important data required. This is commonly a secret phrase, the organization you work for, or bank data. Cybercriminals will figure out their best about you on the web and afterward endeavor to include you as a companion social records. When they get sufficiently close to a record, they can sell your data or secure records in your name.

PUPs: PUPs or Potentially Unwanted Programs are less compromising than different cybercrimes, however are a kind of malware. They uninstall fundamental programming in your framework including web search tools and pre-downloaded applications. They can incorporate spyware or adware, so it's smart to introduce an antivirus programming to keep away from the malevolent download.

Phishing: This kind of assault includes programmers sending malevolent email connections or URLs to clients to get to their records or PC. Cybercriminals are turning out to be more settled and a large number of these messages are not hailed as spam. Clients are fooled into messages guaranteeing they need to change their secret word or update their charging data, giving lawbreakers access.

Prohibited/Illegal Content: This cybercrime includes lawbreakers sharing and disseminating unseemly satisfied that can be viewed as profoundly troubling and hostile. Hostile substance can incorporate, yet isn't restricted to, sexual movement between grown-ups, recordings with extreme rough and recordings of crime. Illegal substance incorporates materials upholding psychological oppression related acts and kid double-dealing material. This sort of satisfied exists both on the regular web and on the dark web, a mysterious network.

Online Scams: These are as a rule as promotions or spam messages that incorporate guarantees of remunerations or offers of unreasonable measures of cash. Online tricks incorporate alluring offers that are "unrealistic" and when tapped on can cause malware to meddle and think twice about.

Exploit Kits: Exploit Kits need a weakness (bug in the code of a product) to deal with a client's PC. They are readymade devices hoodlums can purchase on the web and use against anybody with a PC. The endeavor units are redesigned routinely like ordinary programming and are accessible on dark web hacking discussions.

6. Effect of Cyber-Crime in Personal Life

Cyber-crime is being perpetrated consistently. Criminals carry out cyber-crimes to steal individuals' cash and their personality. With your character, the cyber-criminal: can take out loans, cause credit, gather debt and, then escape suddenly. It can require a long time to restore your personality. A virus can obliterate somebody's records and a lost database can bring about getting undesirable deals calls.

The list below includes some of the most immediate effects:

- lost money due to online theft.
- expenses incurred to fix problems and prevent future cybercrimes.
- loss of reputation due to personal information that is revealed.
- corrupted files due to viruses.
- long-term debt created resulting in poor credit rating due to online identity theft.

Cyber lawbreakers make the most of obscurity, mystery, and interconnectedness given by the Internet, along these lines, going after the actual underpinnings of our cutting-edge data society. Cyber-crime can include botnets, PC viruses, cyber tormenting, cyber following, cyber psychological oppression, cyber erotic entertainment, refusal of administration assaults, hacktivism, fraud, malware, and spam. Policing have battled to stay up with cyber hoodlums, who cost the worldwide economy billions every year. Police are endeavoring to utilize similar instruments cyber lawbreakers use to execute crimes with an end goal to forestall those crimes and deal with the liable gatherings. This article starts by characterizing cyber crime and afterward moves to a conversation of its monetary and social effects. It goes on with point by point outings into cyber harassing and cyber erotic entertainment, two particularly agent instances of cyber crime, and finishes up with a conversation of ways of diminishing the spread of cyber crime.

7. Effect of Cyber-Crime in Corporate World

1) Increased Costs

Companies that want to protect themselves from online thieves have to pull out their wallets to do so. Firms may incur any number of outlays, including:

- Cybersecurity technology and expertise
- Notifying affected parties of a breach
- Insurance premiums
- Public relations support

Ransomware, which can keep laborers from getting to IT frameworks except if the organization takes care of a programmer, can likewise make a significant monetary weight. As indicated by Hiscox, 6% of organizations paid a payoff in 2019, making $381 million in misfortunes. Furthermore, organizations might need to recruit attorneys and different specialists to stay consistent with cybersecurity guidelines. Furthermore, in the event that they're the survivor of an assault, they might need to dish out considerably something else for lawyer charges and harms because of common arguments against the organization.

Equifax, one of the main three credit departments, realized this the most difficult way possible after a 2017 data breach that compromised the individual data of 147 million clients. Because of resulting prosecution, the organization consented to settle up to $425 million to help impacted people.

2) Operational Disruption

Notwithstanding genuine monetary harms, organizations frequently face roundabout expenses from cyberattacks, for example, the chance of a significant interference to tasks that can bring about lost income.

Cybercriminals can utilize quite a few methods for binding an organization's ordinary exercises, whether by tainting PC frameworks with malware that eradicates high-esteem data, or introducing malignant code on a server that squares admittance to your website.

Disturbing the same old thing is the leaned toward device of supposed "hacktivists," who have been known to breach the PC frameworks of government organizations or global companies for the sake of getting down on an apparent off-base or expanding straightforwardness.

In 2010, for instance, programmers thoughtful to WikiLeaks fought back against charge card goliaths Mastercard and Visa by directing assaults that briefly crashed their websites.

3) Altered Business Practices

Cybercrime can affect organizations in something beyond monetary ways. Organizations need to reexamine how they gather and store data to guarantee that delicate data isn't helpless. Many organizations have quit putting away clients' monetary and individual data, for example, charge card numbers, Social Security numbers, and birth dates.

A few organizations have closed down their internet based stores out of concern they can't enough safeguard against cyberattacks. Clients are additionally more keen on knowing how the organizations they manage handle security issues, and they are bound to disparage organizations that are straightforward and vocal about the assurances they have introduced.

4) Reputational Damage

Albeit extreme to completely evaluate, organizations that succumb to bigger cyberattacks may observe their appearance value altogether sullied. Clients, and even providers, may have a solid sense of safety leaving their delicate data in the possession of an organization whose IT foundation was broken no less than once previously.

Retail goliath Target (TGT) saw its standing endure a shot after a 2013 data breach including the charge card data of in excess of 40 million clients, a security disappointment that cost it $18.5 million to settle.

JPMorgan Chase and Co. (JPM) persevered through a comparable bruised eye in 2014, when lawbreakers compromised the data of its financial clients. Programmers accessed the names, addresses, telephone numbers, and email locations of 76 million family records and 7,000,000 independent company accounts.

Notwithstanding decreased institutional trust, research recommends that public corporations are probably going to see a momentary drop in market esteem. Security analysts Comparitech concentrated on 40 data breaches at 34 organizations recorded on the New York Stock Exchange. It observed that the offer costs of compromised organizations fell a normal of 3.5% following an assault, and failed to meet expectations the Nasdaq by 3.5%.

8. Safeguide

1) Multi Factor Authentication

Multi Factor Authentication (MFA) is a confirmation technique that requires the client to give at least two check variables to get to an asset like an application, online record, or a VPN. MFA is a center part of a solid personality and access the board (IAM) strategy. As opposed to simply requesting a username and secret key, MFA requires at least one extra check factors, which diminishes the probability of a fruitful digital assault. Personal Life. The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

2) Software Updates

A considerable lot of the more destructive malware assaults we see exploit programming weaknesses in like manner applications, such as working frameworks and programs. These are enormous projects that require ordinary updates to be careful and stable. So rather than hesitating about programming refreshes, see those updates as one of the most fundamental advances you can take with regards to safeguarding your data.

Notwithstanding security fixes, programming updates can likewise incorporate new or improved elements, or better similarity with various gadgets or applications. They can likewise work on the strength of your product, and eliminate obsolete elements.

These updates are pointed toward making the client experience better. And keeping in mind that rehashed update updates can be irritating, particularly assuming you have many applications, they can work on your involvement with the long run and guarantee that you take full advantage of your innovation.

While some PC programming expects you to physically endorse and introduce refreshes, refreshing programming on your cell phones can be much simpler. You can choose auto-update, guaranteeing that your versatile applications stay current. Taking into account that the normal cell phone proprietor utilizes 30 applications per month, and has something like two times that many introduced, this could save you a great deal of time and exertion.

3) Phishing

To comprehend the life systems of the phishing assault, there is a need for a reasonable and itemized definition that supports past existent definitions. Since a phishing assault establishes a blend of specialized and social designing strategies, another definition (i.e., Anatomy) has been proposed in this article, which depicts the total course of a phishing assault. This gives a superior comprehension to the per users as it covers phishing assaults inside and out from a scope of viewpoints. Different points and this could help novice per users or scientists in this field. To this end, we characterize phishing as a socio-specialized assault, in which the aggressor targets explicit assets by taking advantage of a current weakness to pass a particular

danger by means of a chose medium into the casualty's framework, using social designing stunts or a few different procedures to persuade the casualty into making a particular move that causes different kinds of harms.

9. Conclusion

Cyber security is significant in light of the fact that it includes all that connects with safeguarding our information from cyber aggressors who need to take this data and use it to hurt. This can be delicate information, legislative and industry data, individual data, actually recognizable data (PII), licensed innovation, and safeguarded wellbeing data (PHI).

Having progressed cyber guard projects and components set up to safeguard this information is urgent and to everybody's greatest advantage. Everybody in the public arena depends on basic foundation, for example, clinics and other medical care organizations, monetary help projects, and power plants. We really want these to keep our general public running.

At a singular level, cyber security assaults can prompt fraud and blackmail endeavors, which can cause genuine harm to such person's reality.

We as a whole depend on the security of our information and individual data. For instance, while signing into an application or while filling in additional delicate information in computerized medical services frameworks. If these frameworks, organizations, and foundations don't have the right assurance set up, our information could fall into some unacceptable hands. In this sense, we're discussing insurance as innovation and strategies.

The equivalent goes for associations and organizations, legislatures, the military, and other socially basic associations. They store colossal measures of information in information distribution centers, on PCs, and different gadgets. Quite a bit of this information incorporates delicate data. Openness of this data can by and large be extremely destructive — to resident confidence in foundations, to business seriousness, individual notorieties, and purchaser trust in organizations.

References

[1] https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/

[2] https://ung.edu/continuing-education/news-and-media/cybersecurity.php#:~:text=Since%202013%20there%20are%203%2C809%2C448,every%20day%20reports%20Cybersecurity%20Ventures.

[3] Myriam Dunn Cavelty and Andreas Wenger, Cyber security between socio-technological uncertainty and political fragmentation.

[4] Mariam M. H. Alansari, Zainab Aljazzaf, Muhammad Sarfraz, On Cyber Crimes and Cyber Security."

[5] Perwej, Yusuf & Akhtar, Nikhat & Kulshrestha, Neha & Mishra, Pavan. (2022). A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends. Volume 09, pp, 346-371.

[6] Matthew N. O. Sadiku, Omobayode I. Fagbohungbe, and Sarhan M. Musa Roy, Artificial Intelligence in Cyber Security."

[7] Al-Zahrani, Abdul Rahman, Cyberbullying among Saudi's Higher-Education Students: Implications for Educators and Policymakers. World Journal of Education, vol. 5, 2015.

[8] https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/