Dylan Anderson

211C

Hacking and Cyber-Attacks and Their Effects on the Modern World

I. Introduction

II. General Cyber Attack Methods

   A. How Are These Attacks so Effective?

   B. Effectiveness on Companies

   C. Types of Hackers

III. Government Hacking

   A. Morality and Legality

   B. Hacking Compared to Espionage

   C. Potential Risks

   D. Government Defense Against Cyber Attacks

IV. Public Knowledge and Security

   A. How Can the Public Be Informed?

V. The Impact and Fight Against Cyber Attacks

   A. Cyber Attack Impacts on Economy and Trust

   B. Cyber Attack Impacts on Political Debates and Elections

   C. The Uphill Fight Against Cyber Attacks

VI. Conclusion

Introduction

We now live in an age where almost anything from your tv to your toaster are connected to the internet. This is described as the internet of the things, iot for short (Gillis). In this extremely new age of connectivity, security issues and breaches have become more rampant and more dangerous as time goes on, these being dignified as cyber attacks. Cyber attacks, as the word suggests, are attacks which occur solely digitally through hacking or other malicious ways in search of data, information, or to hold the item at ransom. Hacking, the main form of cyber attacks, are the ways attackers use methods to gain unauthorized access to a server, system, or computer ("What Is a Cyberattack? - Most Common Types"). In our modern era, hacking and cyber attacks are one of the most unnoticed and dangerous foes, posing many risks to personal privacy, data, and economics. However, hacking and cyber attacks in general have become a necessity for companies and countries to gain information and advantages. While cyber attacks and hacking fit such a broad overview of topics and ideas, the four main topics of general cyber attack methods, government hacking, public knowledge and security, and the growing impact and fight against cyber attacks serve to give the easiest and best understanding of the field.

General Cyber Attack Methods

There are many general methods attackers use to gain access to unauthorized data, common types including malwares, phishing, and distributed denial of service attacks. Malware, short for malicious software, is one of the bigger methods of cyber attacks and comes in many different forms. Spyware and keyloggers which can sit undetected for years and seek to only gather information. Ransomware which holds the infected servers data at ransom for a specific price. Viruses which seek to either destroy, steal, or hold data at ransom. These malwares are usually installed through other third party programs or by other attacker methods such as phishing. Phishing is the act of creating fraudulent communications from reputable sources, either through email or other means to steal data. This is usually done through malware installed by a fake link from a message or from downloaded software sent by the attacker through the phishing post. Distributed denial of service attacks, or DDoS attacks for short, flood the traffic of system servers to make them overload and cease functions for periods of time ("What Is a Cyberattack? - Most Common Types").

How Are These Attacks so Effective?

While at first glance most these attacks seem easy to catch and avoid, they usually prey on those without the necessary knowledge to avoid them. Phishing emails for example are usually sent out by the hundreds of thousands, accounting for around almost a billion a day (Palmer). For every person that spots and avoids these usual junk emails, hundreds if not thousands of unknowing people click on these links. This is how general cyber attacks usually function, as a usual scam call, preying on those who don't understand what they're getting themselves into. DDos attacks are usually not used in general methods of attack as they are complete server shutdowns instead of any information gathering, and are extremely expensive.

Effectiveness on Companies

While it’s hard to believe, companies are extremely susceptible to these types of general methods of cyber attacks as well. This is due to the lack of company training on how to deal with these issues effectively. Due to the relative modernity of cyber attacks on a wide spread level, companies have not adapted their cybersecurity training policies to where they should be. Also, these types of general attacking methods are on a much higher and direct scale. A phishing link may have the exact company logo or be made to look like an employee of a company, match this with employees working in a hasty environment where there isn’t much time to thoroughly read every email, it’s not hard to see why these attacks still happen so often.

Types of Hackers

There are three main types of hackers, white hat, grey hat, and black hat hackers. White hat or ethical hackers are considered the good types of hackers usually in government or security positions. These types of hackers usually follow the rules when breaking into systems and obey the necessary disclosure laws, usually doing nothing harmful and instead fixing the found flaws. Grey hat or vigilante hackers are in between white and black hat hackers. These types of hackers may have good or bad intentions, and may not disclose the necessary fixes for the system breached, and usually prioritize personal feelings over the law. Black hat or criminal hackers are considered the main cybercriminals. These types of hackers do not care about legality and use the cyber attack methods for personal or political gain (“Black Hat, White Hat & Grey Hat Hackers - Differences Explained”).

Government Hacking

In the modern era, hacking and cyber attacks have become the main type of warfare for governments in order to gain advantages and information on other countries. However, due to the moral grey area and potential risks of war of outing themselves as cyber attacks, most governments do not show off these actions to the public. Cyber attacks and hacking in general have become a necessary evil to most governments that cannot be accurately researched to the fullest extent due to the high classification of these potential attacks and the risks they may cause.

Morality and Legality

The action of hacking and accessing unauthorized data has a strict illegal undertone to it, to where most governments define hacking or cyber attacks as highly illegal crimes which can result in severe penalties ("Unauthorized Computer Access (Otherwise Known as Hacking)"). While most governments define cyber attacks and hacking as illegal, most governments also participate in these hacks themselves creating a moral gray area. Governments such as the U.S. and China have been known to invasively spy on their own citizens, with the U.S. NSA having a gigantic scandal which leaked how almost all Americans personal information was intercepted and stored by their own government (Greene et al.). The moral gray area constructed by these governments under the pretense of upholding national security is exactly where hacking and cyber attacks stand in government use, and will most likely stay that way until they are either leaked or declassified.

Hacking Compared to Espionage

The way hacking is used in government can be compared to how espionage has been used throughout most of all government's existence. Espionage, another illegal but widely used tactic by most governments, seeks to learn hidden information about other countries or figures to gain advantages ("Espionage Definition & Meaning"). These tactics all serve the same purpose to gain information and advantages, hacking and cyber attacks are the more modern day easier methods than traditional acts of espionage.

Potential Risks

There are a wide variety of risks that come with government hacking compared to the types of information gathering used prior. Hacking an encrypted system enough to break into the system in question can leave it damaged or more exploitable to those with more nefarious intentions. Most government agencies purchase or hire hacking companies to break into these cases, these companies can sell the same exploitation methods to other entities and also sell highly classified government secrets depending on their relationship with the government in question. The exploitation methods by these companies and governments, if studied enough, can be replicated, stolen or modified to fit the needs of those who would use the methods for more evil purposes. Government hacking can also turn one specific target into multiple with one code, leading to potentially devastating scenarios ("Fact Sheet: Government Hacking"). The Stuxnet virus for example, which was allegedly created by the United States and Israeli governments to destroy Iranian nuclear centrifuges ended up spreading around the globe and infecting millions of other systems (“What Is Stuxnet?”). The biggest threat to government hacking of other foriegn nations however is the potential to spark war. All forms of hacking to gain access to unauthorized information are considered attacks no matter how small they might be, if one struck a particular cord to a different nation, an all out war could be started by one attack.

Government Defense Against Cyber Attacks

Government defense, while not being able to fully prevent all cyber breaches, helps to minimize the possibility of these breaches occurring to a minimum. Necessary government funding and training of employees to protect themselves against common cyber attack methods goes a long way. As it stands, the countries and governments with the most wealth usually have the necessary funding to actively fight and defend against oncoming cyber threats, it’s just lack of proper funding towards these which causes the sheer amounts of breaches occurring. As an example, the United States, one of the global superpowers, had an astonishing 6551 breaches from 2013-2017, over 1000% more than second place, the United Kingdom with 570 breaches (“Data Breach Statistics: by Source, Industry, Country & Size”).

Public Knowledge and Security

Public knowledge about cyber breaches and hacking in general is very limited. In a study done in 2017 by Pewresearch, the general public was able to answer less than half, around two of the thirteen questions provided. The two questions that were answered were very trivial about password strength and safety of public wifi networks, but around nothing else (Smith). It is safe to say public knowledge on these issues is extremely limited to what it should be. This is due to the relative new age of the internet and the implementation of the internet of things being so widespread, almost anywhere is a hotspot, but almost nothing is given to the public. Due to the limited amount of knowledge and information about cyber attacks, hacking, and cybersecurity in general, it's no wonder why security against these attacks is so nonexistent. The main forms of protection the public is told is to create stronger passwords, and to beware of fake emails. The public also uses general tools such as antiviruses and constant updates to protect themselves against malware, however these sometimes do not protect against some attack methods and breaches.

How Can the Public Be Informed?

While nowadays cyber attacks and hacking are becoming more of a widespread issue and more people are becoming aware of them, governments and media can still do more of a part to inform their citizens on cyber attacks and hacking. The media can inform the public more widespreadly through social media and the news to help less educated citizens learn about the dangers of cyber attacks and hacks. Government institutes such as the National Institute of Science and Technology (NIST) have dedicated the month of October to cybersecurity awareness (Koziol). These awareness months could be more marketed and widespread to the public to increase knowledge and therefore more security.

The Impact and Fight Against Cyber Attacks

Cyber attacks are one of the most rapidly growing and dangerous predicaments of our modern times and are currently unmanageable by the current forces allocated to it. Cyber breaches occur every single day, with millions already being breached but not known or reported ("What Is a Cyberattack? - Most Common Types"). In a 2020 study, 78% of works lack confidence in their company's cybersecurity posture, around 80% of senior IT workers and security leaders believe their company lacks sufficient protections against cyber attacks, on the opposite side, identity theft cases in the pandemic doubled to 1.4 million reports, the average cost of a data breach is $3.86 million, malware increased by 358% in 2020 alone, and ransomware victim every 10 seconds (Brooks). These studies from the most recent year alone paint a very dark future for the future of information and the public. Cyber attacks also impact countries both economically and politically.

Cyber Attack Impacts on Economy and Trust

Data breaches being so much more rampant this year and continuously growing make the costs of data breaches more and more hindersome. While the average cost of a data breach is $3.86 million, this is just the average. Some bigger breaches of data could cost companies upwards of 50 to a 100 million which could almost destroy some smaller companies. These economic costs don't just affect corporations however, these cybercrime costs are expected to rise $10.5 trillion annually by 2025 (Brooks 2021). These rampant breaches also cause distrust between companies and consumers as data breaches are sometimes kept under wraps by companies. One of the biggest examples of this was a very recent breach on Facebook in which 533 million users' phone numbers and personal data was leaked online. This personal information included full names, addresses, email addresses, and biological information, all of which could be used for identity theft. The biggest issue of this breach was the initial date of the breach was in 2019 but was not made public until 2021, two years after the incident occurred (Holmes). If a breach of this magnitude took two years to be discovered by the public, how many other gigantic breaches are being held by companies to not cause panic or keep public support. Just the mere thought of breaches serve to create massive distrust between consumers, companies, and governments.

Cyber Attack Impacts on Political Debates and Elections

Cyber attacks, breaches, and then leaks can cause extreme shifts in political debates, elections, or the general press. No bigger example of this occurred than in the 2016 U.S. Democratic National Committee email leak. These emails contained information on alleged bias against president campaigner Bernie Sanders against the publicly stated neutrality of the DNC. These email leaks resulted in the resignation of the DNC chair Debbie Schultz, and a formal apology from the DNC to Sanders. The breach was determined by the U.S. to have originally come from Russia. The outward negative public reaction towards Democratic nominee Hillary Clinton after these email leaks were a contributing factor to the eventual win by Republican Donald Trump for the presidential spot (“Democratic National Committee (DNC) email leak, 2016”). If this leak had never occurred at the time it did or at all, it’s likely to say the winner of the presidential election may have been different. Cyber attacks and the information leaked from these breaches being placed into the public can drastically sway outcomes and public opinion for better or worse.

The Uphill Fight Against Cyber Attacks

As it stands now, the cybersecurity field is extremely underprepared to deal with the behemoth of cybercrime. With the internet of things expected to increase to 35 billion in 2021 and 75 billion in 2025, it’s only going to get worse (Brooks). The entire cybersecurity field is extremely saturated with about 500,000 open jobs across the economy (Carino). While technology grows cybercriminals have the edge, the global pandemic of cybercrime grows each year, but can be defeated with enough effort. As said before, most of the back end of cybercrimes are on low end scales like phishing and low grade malware, which are entirely preventable. As the modern world becomes more aware of cybercrime it’s up to those with the knowledge to educate those without to create a more secure world.

Conclusion

In conclusion, cyber attacks and hacking, the main method of these attacks, are an unspoken pandemic which plagues the modern world. In order to accurately understand cyber attacks and hacking at their most basic forms, four main topics allow for the most easy to digest and understand view into the world of cybersecurity; general cyber attack methods, government hacking, public knowledge and security, and the growing impact and fight against cyber attacks. Most cyber attacks and hacks generally work off a low end structure which can be prevented with enough widespread public knowledge and security tips. The unspoken pandemic of cybercrime is currently a behemoth that is constantly growing after each and every year, however it can still be fought and prevented if enough information is raised. The biggest issue of cybercrime is the rapid growth of the internet of things, with current cybersecurity fields not being funded and staffed enough to deal with the gigantic problem at hand. Mix this with limited public knowledge on the true dangers of cybersecurity, and there's no wonder why this problem has grown into the pandemic it is. This unspoken pandemic can still be managed with enough funding and effort, the cybersecurity field is extremely saturated and needs all the help it can get to stop this monster. All it takes is a little awareness and knowledge on everyone’s part.

References

"Black Hat, White Hat & Grey Hat Hackers - Differences Explained." *Norton*, 24 July 2017, https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html.

Brooks, Chuck. "Alarming Cybersecurity Stats: What You Need To Know For 2021." *Forbes*, Forbes Magazine, 3 March 2021, https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/.

Carino, Meghan McCarty. "White House seeks to plug cybersecurity job hole." *Marketplace.org*, 25 August 2021, https://www.marketplace.org/2021/08/25/white-house-seeks-to-plug-cybersecurity-job-hole/.

"Data Breach Statistics: by Source, Industry, Country & Size." *Apcela*, 19 November 2018, https://www.apcela.com/blog/data-breach-statistics/.

"Democratic National Committee (DNC) email leak, 2016." *Ballotpedia*, https://ballotpedia.org/Democratic_National_Committee_(DNC)_email_leak,_2016.

"Espionage Definition & Meaning." *Merriam-Webster*, https://www.merriam-webster.com/dictionary/espionage.

"Fact Sheet: Government Hacking." *Internet Society*, 29 May 2020, https://www.internetsociety.org/resources/doc/2020/fact-sheet-government-hacking/.

Gillis, Alexander S. "What is IoT (Internet of Things) and How Does it Work?" *IoT Agenda*, 11 Febuary 2020, https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

Greene, David, et al. "NSA Spying." *Electronic Frontier Foundation*, https://www.eff.org/nsa-spying.

Holmes, Aaron. "Stolen Data of 533 Million Facebook Users Leaked Online." *Business Insider*, Business Insider, 3 April 2021, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

Koziol, Jack. "Cybersecurity Awareness: What It Is And How To Start." *Forbes*, Forbes Magazine, 27 October 2021, https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/.

Palmer, Danny. “Three billion phishing emails are sent every day. But one change could make life much harder for scammers.” *ZDNet*, 23 March 2021, https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/.

Smith, Aaron. “What Americans Knows About Cybersecurity.” *Pew Research Center*, Pew Research Center, 22 March 2017, https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/.

“Unauthorized Computer Access (Otherwise Known as Hacking).” *Law Offices of Seth P. Chazin*, https://www.bayarea-attorney.com/unauthorized-computer-access-otherwise-known-as-hacking.

“What Is a Cyberattack? - Most Common Types.” *Cisco*, 28 September 2021, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

“What Is Stuxnet?” *McAfee*, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.