IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

Future Crime in Cyber Security

Pratik Shah[1], Vansh Damania[2], Hitansh Kadakia[3]
Lecturer, Department of Computer Science[1]
Students, Department of Computer Science[2,3]
Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India
pratik.shah@sbmp.ac.in[1], vanshdamania@outlook.com[2], hitanshchiragkadakia@gmail.com[3]

Abstract: *As we all know nowadays everything is connected to the internet. Bits and bytes flow freely from one country to another country without any border guards. Technology progress has helped our world in many ways, but there are always two sides to everything. where there are good things. there are bad things also. In today's society, we spend the majority of our time online, be it doing business, paying bills, making friends, selling cars, or purchasing a home, from applying to college to finding a life partner. Today's criminals are taking the advantage of technology for crimes. The most often asked question is "What is the next big crime?" the answer in this paper. We covered some worst scenarios/cybercrimes you've never thought of. Before you begin with this paper, let us first tell you what this paper is not. It is not a guide on how to hack someone's social media accounts, mobile devices, etc., or how to prevent yourself from hackers or cybercriminals. Yes, we covered some prevention techniques but, in the end, it all depends on you. This paper isn't just what was going on yesterday or even what Is happening today. It is about where we are going tomorrow. This research paper throws light on the field of cybercrimes which are usually people don't know.*

Keywords: Hacking, Cyber Security, Cyber Crime, eSIM Fraud, Salami Attack, Dark Web, Hit Men Services, Bait Switch Attack, Car Hacking.

I. INTRODUCTION

Nowadays all people know what is hacking, but do you know the origin of hacking? So let us tell you a little bit about hacking origin and the keys that are connecting dots in the world of hacking. Hacking is carried out in the 1960s by some MIT engineers. There are working on some kind of harmless technical activity as part of the research just to give the assignments and their outcomes a little funny and faulty. then playing for a little while from these flaws they have a term these flaws as hacks. So even before the internet was born several people in the US started finding flaws to get some benefits. like the first thing they did is modify the telephones to make long-distance phone calls over the phone network illegally and nowadays with a little bit of modification IOT hacking is done for which hacking world getting crazy these days.

1.1 What is Hacking?

Hacking refers to the hobby/profession of accessing a computer system without the permission of the owner of that system [8]. or more commonly it refers to breaking into the computer system.

1.2 What is Cyber Crime?

Cybercrime is any criminal activity that involves a PC, laptop, and network [1]. As per the definition, cybercrimes would mainly be restricted to tampering with the PC or laptop source code, hacking and cyber pornography. cyber fraud, defamation, harassment, e-mail abuse, etc. Clearly, cybercrime can be called a commission act or omission, committed, or committed, or with the help of an internet connection, whether directly or indirectly. Okay, a pretty much good information about the basic concept. Coming to the main topic now days cybercriminal constantly updates their techniques and tricks to include the very latest emerging technologies into their Modi operandi. We use various

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

technological tools to build our society, but the same thing can be used against us. The more we plug our lives and device into global information the more vulnerable we become.

II. Cyber Crime Rate Increase Due To Covid 19

The lockdown due to COVID 19, has led to more people being online at home and increasingly depending on the Internet to access services. The dangers of cyber-crime have been there for many years, but the increase in the population connected to the Internet has provided more opportunities for cybercriminals to take advantage of the situation and make more money or create a disturbance on the internet. Some vulnerable segments of the such as children more time online for education [2]. This sudden change in how we live our lives and use the Internet has prompted a rapid increase in e-crimes.

III. ESIM Fraud

eSIM is a new service for mobile users to stay away from the need for a physical sim. Nowadays, this service is given by all the telecom operators [6]. This is a new technology and most people are not aware of it. cybercriminals are taking advantage of these services. They are making a call saying ”Your SIM card verification is due coming. If you have not verified your SIM card in 24 hours your SIM card will be blocked permanently”. and then they teach all the steps to take. Basically, cybercriminals made you prey to eSIM swapping. The criminals got another SIM issued in place of yours. and using that SIM cybercriminals can hack your all social media accounts, bank accounts. Your full identity will be completely in their control.

IV. Salami Attack

A salami attack is a criminal’s attempt to withdraw small amounts of money from the accounts of different victims so that he cannot be detected. Hackers use it as a very safe tool to get a large amount without being recognized. The crime of identity theft, fraud, and EDI is almost identical when criminals steal data using fraudulent tactics. He may act as an intermediary while communicating between the consumer and the bank and stealing information by acting on the web. and the bank also steals information by hiding it on the web [5].

V. Inside The Digital Underground

The dark web is a part of the internet that isn’t accessed by normal search engines. Dark web is a place where many criminal activities take place. Almost 57 percent of websites on dark web are illegal You can buy all manner of drugs, credit card numbers, guns stolen subscription credentials, counterfeit money, hacked Netflix accounts and software that helps you break into other people’s computers [4]. Buy login credentials to an any Bank account, counterfeit dollars 20 bills, prepaid debit cards, or a “lifetime” Netflix premium account. You can also hire hackers for you. You can buy usernames and passwords. and many more.

VI. Hit Men Services

Tor - The Onion Router, a software tool that provides the closest thing to actual anonymity on the internet. Tor works by routing your Web connections through a worldwide array of your connection. By using TOR only you can access DARK Net [7]. Service providers such as Killer for Hire, Quick Kill, Contract Killer, and all advertise ”Permanent solutions to common problems”. Each service has different rules and regulations. One has a strict ”no minors policy” and refuses to murder children under eighteen, while another demurs when it comes to political assassinations. No worries, though, there are just as many services that are dedicated to killing government officials [3]. Price ranges from a low of Dollar 20,000 to more than 0ne lakh dollars to kill a police officer. These sites request you provide a recent photograph of the target, as well as home and work address, daily routines, and frequent hangouts. Bitcoin gladly accepted, and photographic proof of murder is included standard. attackers substitute an innocuous link with the ad, which could be used later to download malware or browser locks or to compromise the targeted system. In some cases, the ad may also link to a proper website, but it to a far more harmful site[10].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

VII. Bat And Switch Attack

Bait and Switch is a type of fraud that uses trusted avenues ads to trick users into visiting malicious sites. This often occur in the form of advertising space being sold by websites and purchased by attackers. Once they purchase the ad, the A.

VIII. Car Hacking

Previously, cars ran on gasoline. today then run on code. Sure, you still need gas or electricity for power, but without functioning computer code any modern car is dead in its tracks. Using nothing more than a laptop and an SMS text message with the correct encoded instructions, thieves can unlock your doors, start the car and drive off [11]. As several security researchers demonstrated in 2011, you are at risk if you enjoy listening to music, since malicious code can be added to an MP3 and it is burned to a CD. When played through the car's audio system, the infected song file warped the vehicle's firmware, allowing hackers entry to all the car's main control system [12]. Car theft might actually be the best outcome in these circumstances since once the onboard computer systems of a vehicle are compromised, the possibilities are almost limitless.

IX. 3D Printers Can Deliver AK-47

3D printing or as it is sometimes called additive manufacturing. At a push of a button, a magical machine can make physical objects before your very eyes using a wide array of materials, including plastic, metal, wood, concrete, ceramics, and even chocolate. Just as you can send a photograph to your 2-D inkjet printer, so too can you download or create a design on your laptop and send it to a 3-D printer, which uses a variety of techniques, can build objects in three dimensions, layer by layer, with incredible precision [13]. Nowadays 3-D can easily deliver weapons. It's nearly impossible to detect these plastic firearms on standard metal detectors, as Israeli reporters proved by smuggling a 3-D printed gun into the highly secure Knesset building twice [14]. Repositories are easily available for 3-D weapons that have been created, including those that have plans for hand grenades and mortar rounds. The FBI's Terrorist Explosive Device Analytical Center is concerned about the train and recently purchased its own 3D printer for investigating how terrorists might use 3D printers to build IEDs [15]. This challenge 3D printing poses to international security. and 3D printed weapons are de facto banned because the law bans all manufacturing [16].

X. Prevention

10.1 Encryption

Encrypt your digital life, and keep track of your data at leisure and across the web. Both Windows and Mac include free full-fragment encryption programs (Birl. Ocker and Fil-eVault, independently). Breaking your database means that others cannot read its contents if it is lost or stolen. You should also hide your online business using a virtual private network (VPN), especially if you use a public Wi-Fi network such as the one for airports, universities, conferences, and regular coffee shops targeted at criminals and thieves. Your phone needs to be translated because the temporary bias of the phone may contain some important information such as laptops, if not. Always use the name on your cell phone, and consider enabling biometric security, such as Apple's Touch ID printing technology. Using the name in the background description of iOS and Android not only ensures that no alternative can pierce your phone and its data when you are not there but also provides full encryption to the device, adding another level of capture and security.

10.2 Administrator

Administrator accounts should be used with care. Both Windows and Apple allow druggies to set account boons, with administrators having the loftiest boons. While you'll need an administrator account on your computer, it shouldn't be your dereliction account for everyday work and online browsing. Rather, produce a standard stoner account to do the maturity of your work and for day-to-day use. When you're logged in under executive boons and accidentally click on an infected train or download a contagion, the malware has full boons to execute and infect your machine. However, frequently the contagion, Trojan, If you're logged in as a general stoner and the same thing happens. Always run your

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

computer as an anon-admin stoner unless absolutely necessary to carry out a particular task, similar to a known update from a trusted source you're rigorously installing.

10.3 Password

Password should be long (suppose twenty integers or further) and contain upper and lowercase letters, as well as symbols and spaces, Though we have all heard it a million times, the strength of a password is one of the crucial factors in guarding your accounts, and password should be changed frequently. You should absolutely not use the same word for several different spots, Doing so means once hackers get access to your log-in credentials, they can use them across multiple disciplines, from your social media network to your bank account. Learning long, unique password for every account and Web point in your life, still, is of course further than the mortal mind can manage. Fortunately, there is a bevy of words" holdalls" or directors that can make this process fairly effortless. Culprits have been known to produce their own word holdalls in trouble to trick you into giving up your digital crown jewels. Therefore use only well-known and established companies similar as 1Password, LastPass, KeePass, and Dashlane, utmost of which work across your computer, smartphone, and tablet. In addition, numerous services similar to Google, iCloud, Dropbox, Evernote, PayPal, Facebook, LinkedIn, and Twitter offer two-factor authentication, which involves transferring you a separate onetime word every time you log on, generally via an SMS communication or app directly to your mobile phone. Using two-factor authentication means that indeed if your word is compromised, it cannot be used without the alternate authentication factor (physical access to your mobile device itself).

10.4 Update Constantly

Ultramodern software programs are riddled with bugs. Hackers and others use these vulnerabilities to break into your computer and other bias, steal your plutocrat and beget general annihilation. Avoid these problems by automatically stream-lining your operating system software, computer programs, and apps. Pay particularly close attention to cybersurfers, plug- sways, media players, Flash, and Adobe Acrobat-favorite targets of bad guys trying to rip you off. Failing to modernize automatically leaves your bias wide open to attack via problems that can be avoided if you simply update your software.

XI. SURVEY

We did a small survey of cybersecurity. The main goal of this survey was to see how many people know about cybercrime, what do they think about it and most importantly was to know the types of crimes which are common in their area. Data collected are from students, people working in IT corporations as well as those who are working in a different area than IT.

Figure 1: Survey Question About Those Who Knows About Cyber-Crime.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

Figure 2: Survey Question About Type of Attacks that People are Facing.

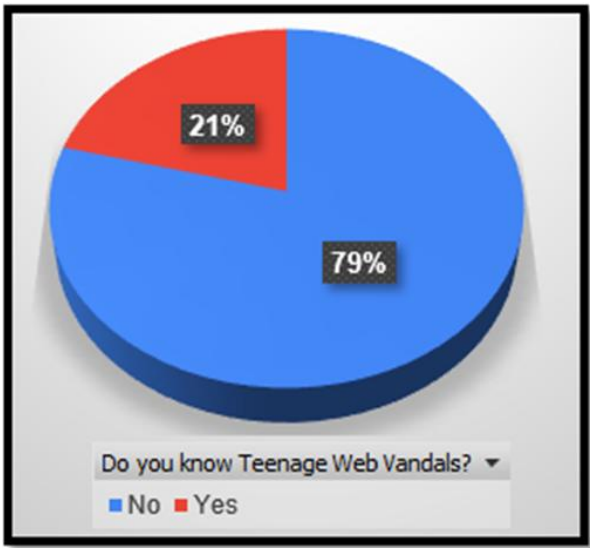

Figure 3: Survey Question About Those Who Knows About Teenage Web Vandal.

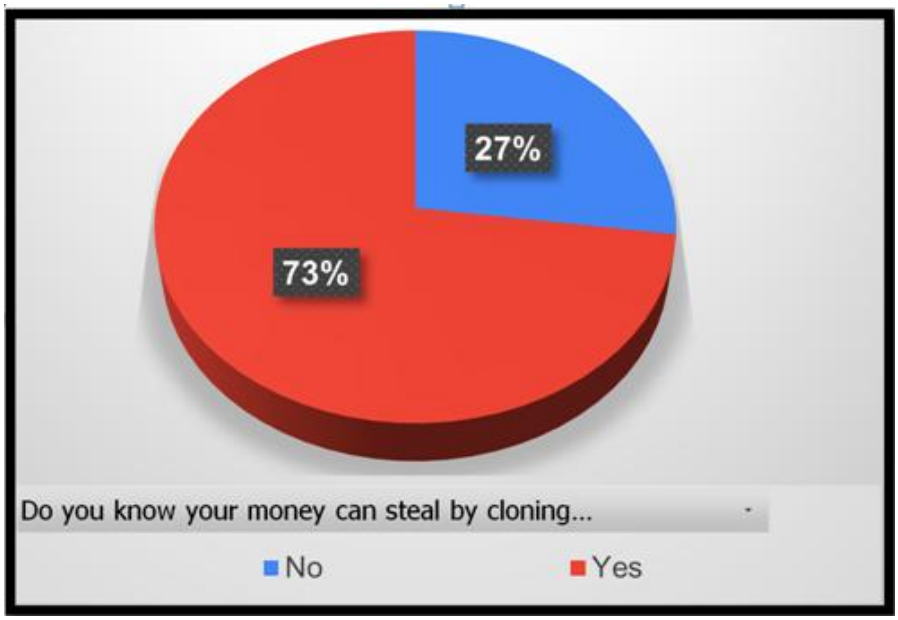

Figure 4: Survey Question About Those Who knows About Money can steal by cloning fingerprints.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

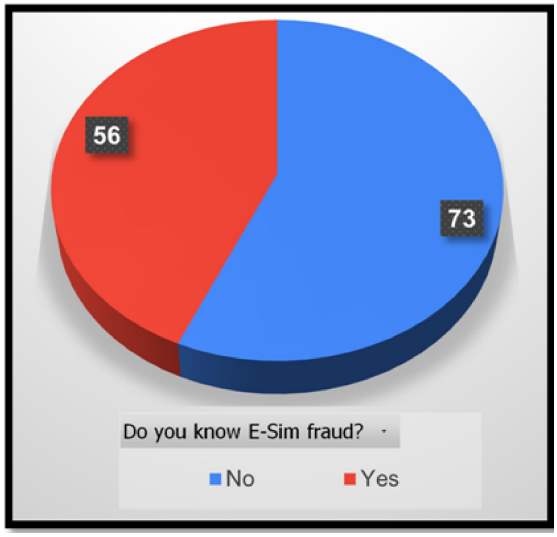

Figure 5: Survey Question About Those Who Knows About eSIM Fraud.

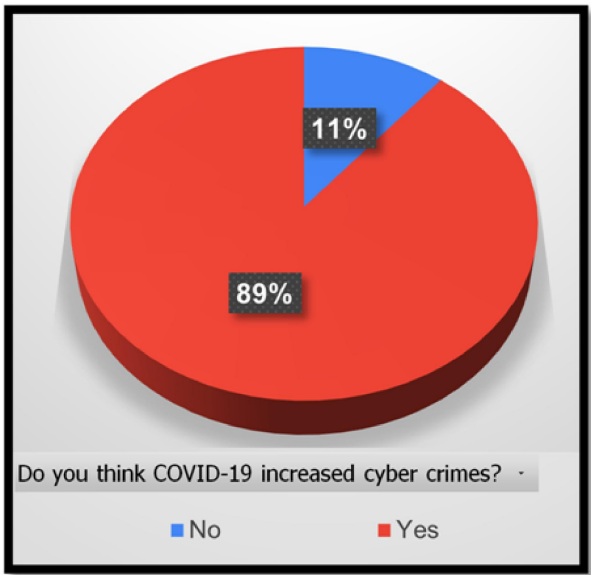

Figure 6: Survey Question About Those Who Thinks COVID-19 can increase cyber crime.

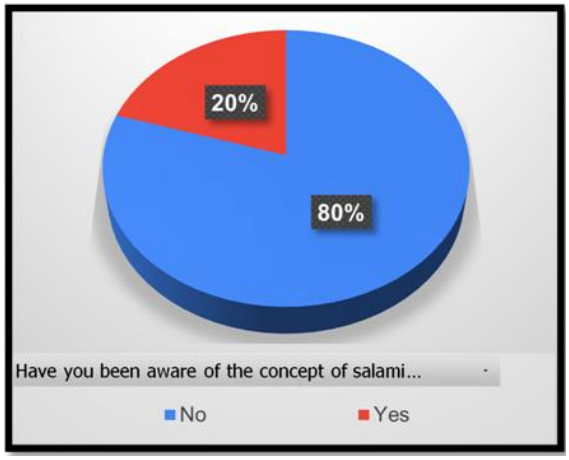

Figure 7: Survey Question About Those Who Knows About Salami Attack.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

This survey helps us to have an idea about the types of cyber-crimes that people and organizations are facing. The vast majority of people are unaware of crimes that are happening, as well as actions needed to bring more security to alarming areas.

XII. ACKNOWLEDGEMENT

We would like to express our deepest gratitude to our mentor, Mr. Pratik Shah for his constant support and guidance throughout the process of articulating this paper. We would also like to say a very sincere thank you to Marc Goodman, author of the Future Crime series. The ideas for this paper were drawn from Marc Goodman's books. We borrowed some methods and prevention techniques from his book [17]. We also want to thank our peers for helping us in improving the quality of the paper.

XIII. CONCLUSION

In our paper, all the attacks that have been mentioned are not it, there are many more that most of the people are not aware of. Hence through our paper we have tried our level best to make the people aware by mainly following 2 things At the first getting regularly updated with the newer technologies and secondly surfing through the web safely. If an individual keeps these 2 things in mind, it will help them be safe and protected. As we discussed all the crimes, these activities can be eradicated with appropriate measures. and as we look ahead toward the future of crime, two things are becoming apparent: the future of cybercrime will be exponential and automated. We need to become aware of the growing rates of cybercrime and learn more about it. We must have to keep updating ourself. [2]

REFERENCES

[1]. Cisco. What Is Cybersecurity? https://www.cisco.com/c/en in/products/security/what-is-cybersecurity.html.
[2]. Cyber-crime during the COVID-19 Pandemic. http://f3magazine.unicri.it/?p=2085. 2020.
[3]. Andy Greenberg. "Meet the 'assassination market'creator who's crowd funding murder with Bitcoins". In: Forbes, November 18 (2013), p. 2014.
[4]. Darren Guccione. What is the dark web? How to access it and what you'll find. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html. 2022.
[5]. The Economic Times. IT Act to get more teeth to fight financial frauds. https://economictimes.indiatimes.com/tech/internet/it-act-to-get-more-teeth-to-fight-financial-frauds/articleshow/2656537.cms?utm source=contentof interest utm medium = text & utm campaign= cppst. 2007.
[6]. TIMESOFINDIA.COM. e-sim fraud: Government has an advisory on how not to fall for e-SIM registration frauds
[7]. Times of India. https://timesofindia.indiatimes.com/gadgets- news/government- has- an- advisory- on- how-not- to- fall - for- e- sim- registration- frauds/articleshow/78423784.cms. 2020.
[8]. Tor. The Tor Project — Privacy Freedom Online. https://torproject.org.
[9]. Lawrence Williams. What is Hacking? Types of Hackers— Introduction to Cybercrime. https://www.guru99.com/ what-is-hacking-an-introduction.html.
[10]. Labs, Cyware. "What Is Bait & Switch Attack and How Is It Different from Clickjacking? | Cyware Hacker News." Cyware Labs, https://cyware.com/news/what-is-bait-switch-attack-and-how-is-it-different-from-clickjacking- d33b450a.
[11]. How to Unlock a Car with a Text Message. http://www.cnn.com/2011/TECH/mobile/08/03/black.hat.war.texting/index.html.
[12]. Your musical tastes: Rebecca Boyle, "Torjan-Horse MP3s Could Let Hackers Break Into Your Car Remotely, Research Find," Popular Science, March 14, 2011.
[13]. Clinch, Matt. 3-D printing market to grow 500% in 5 years. (2014).
[14]. Greenberg, Andy. How 3-D printed guns evolved into serious weapons in just one year. Wired. Retreived from http://www. wired. com/2014/05/3d-printed-guns (2014).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

[15]. Sternstein, A. The FBI is Getting Its Own, Personal 3D Printer For Studying Bombs; Accessed: Mar 30 (2015): 2016.

[16]. "3D Printed Firearm." Wikipedia, 1 Dec. 2021. Wikipedia, https://en.wikipedia.org/w/index.php ?title=3D_printed_fir earm;oldid=1058160039.

[17]. Goodman, Marc. Future Crimes: Everything is Connected, Everyone is Vulnerable and what We Can Do about it. United States, Doubleday, 2015.