IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

A Review on Different Ethical Hacking Techniques and its Impact on Cyber Security

Purva Vijay Patyane and Vibha Kenny
Students, Master of Computer Application
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *A person engages in hacking when they take advantage of a system's flaw for their gain or satisfaction. A similar activity known as "ethical hacking" tries to identify and fix a system's weaknesses. Computer security is of the utmost concern to organizations and the government in the era of the Internet. These businesses use the Internet for a huge range of purposes, including electronic commerce, marketing, and database access. Data and network security, however, is a critical issue that has to be discussed. This paper tries to go through the basics of hacking and how ethical hacking compromises security. Additionally, there are differences between malicious and ethical hackers as well as their respective roles in security. To increase their aptitude and ability to multitask, specialists who use their talents to redevelop mainframe systems are referred to as hackers. Nowadays, the phrase is often used to characterize talented programmers who, driven by malice or mischief, exploit loopholes or use defects to obtain unauthorized access to computer systems. For instance, a hacker can create algorithms to break networks, compromise networks, or even impair network services. Theft of priceless records or financial gain is the main reason for harmful or unethical hacking. But not all hacking is bad anymore. This brings up a different kind of hacking: Hacking with integrity*

Keywords: Ethical hacking, hacker, authorized, system, hacking, secure, passwords, Access, weaknesses

I. INTRODUCTION

Navigating system security to find possible network threats and data breaches is a legal practice known as ethical hacking. To test the system's defenses, the system or network's owner firm permits cyber security engineers to carry out such exercises. As a result, this process is organized, acknowledged, and notably legal, unlike malevolent hacking.

Ethical hackers aim to examine the system or community for weak points that bad hackers could exploit or harm. To parent out strategies to strengthen the security of the system, device, network, and applications, they keep in mind and compile the data. By doing this, companies might improve their security footprint and better deflect or withstand assaults and attacks.

Organizations hire ethical hackers to investigate the vulnerabilities of their systems and networks and design solutions to prevent data breaches. Consider it a high-tech twist on the adage, "It takes a thief to catch a thief."

As computer technology grows, its darker side—HACKERS—also emerges likewise. Data security is a big problem in the modern world, since the internet is expanding so quickly and so much data, is flowing online. The danger to data security has increased as a result of the increased digitalization of many operations, including banking, online transactions, online money transfers, and online sending and receiving of many types of data. These days, a big number of businesses, organizations, banks, and websites are the targets of numerous hacking assaults. In general, when we hear the term "hacker," we all picture horrible persons with evil intentions who are experts in computers and try to steal, someone with malicious intent who tries to steal, leak, or destroy another person's sensitive or valuable data without that person's knowledge. They are the individuals with incredibly advanced computer skills who attempt to breach another person's security to get their data, however, this rarely happens. We have ethical hackers in the sector, who are also computer experts like the hackers but with good intentions or constrained by some set of rules and regulations by the various organizations, to reduce the chance of being hacked by hackers. These are the people who work to keep the owner's data safe while attempting to defend it against various hacker attacks. Additionally, this essay explains more.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

Key Ethical Hacking Principles:

- **Stay Legal.** Obtain proper authorization before entering and executing security assessments.
- **Establish the scope.** Determine the scope of the assessment so that the ethical hacker's work remains legal and within the corporation's approved parameters.
- **Identify and report vulnerabilities.** The organization should be informed of any vulnerabilities discovered throughout the assessment.
- **Be mindful of data sensitivity.** Depending on the data disclaimer contract, as well as any extra limitations or limits imposed by the evaluated organization.

II. LITERATURE REVIEW

Ethical hackers use their expertise to protect and advance an organization's technology. By checking for security threats that could arise from vulnerabilities, they offer an indispensable service to organizations.

An ethical hacker reports discovering vulnerabilities in the organization. They also offer remediation guidance. In many cases, with the organization's approval, the ethical hacker re-tests to ensure that the vulnerabilities are completely patched.

Malicious hackers want unauthorized access to a resource (the more sensitive, the better) in exchange for monetary gain or personal recognition. Some malicious hackers deface websites or destroy backend systems for pleasure, reputational injury, or monetary loss. The methods employed and vulnerabilities discovered remain unreported. They aren't interested in improving the organization's security posture.

III. TYPES OF HACKERS

Based on their motivation for hacking a system, hackers can be divided into numerous categories such as white hat, black hat, and grey hat. These expressions are based on vintage spaghetti westerns in which the villain dons a black cowboy hat while the hero dons a white one.

3.1 White Hat Hackers

White hat hackers also go by the name of ethical hackers. As part of penetration testing and vulnerability assessments, they never intend to harm or damage a device; instead, they seek to identify areas of vulnerability in a computer or network system. One of the most difficult tasks in the IT business is ethical hacking, which is legal. For vulnerability analysis and penetration testing, several businesses use ethical hackers.

3.2 Black Hat Hackers

Black Hat hackers, often known as crackers, are individuals who hack into a system without authorization to disrupt its operations or steal sensitive data. Because of their nefarious intent, which includes stealing company data, violating privacy, damaging systems, preventing network connectivity, and other things, their operation is always illegal.

3.3 Grey Hat Hackers

Cybercriminals who use both black hat and white hat tactics are known as grey hat hackers. They do so without the owner's knowledge or permission, but they do so out of amusement and to take advantage of a security flaw in a computer system or network. The owners' admiration, a small gratuity, or an endowment are what they are after in exchange for bringing up the weak spot.

3.4 Red Hat Hackers

In addition, red hat hackers are a combination of both black hat and white hat hackers. They typically focus on the depths to which government organizations, top-secret information hubs, and typically something that falls under the category of crucial data or information, have been hacked.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

3.5 Blue Hat Hackers

A blue hat hacker is a person who conducts evaluations of systems before their deployment outside the scope of computer security consulting firms. They aim to seal any holes in the system where they can affect it. Microsoft also refers to a series of security briefing sessions as Blue Hat.

3.6 Elite Hackers

The most skilled are referred to by this social rank among hackers. These hackers will share recently found exploits.

3.7 Script Kiddie

The term "kiddie" is used to characterize a non-professional who uses pre-packaged automated tools created by others, typically with little comprehension of the underlying concept, to break into computer systems.

3.8 Neophyte

A novice, also known as an "n00b," "newbie," or "green hat hacker," is new to hacking or phreaking and has little to no knowledge of how technology works.

3.9 Hacktivist

A hacker who uses technology to spread a social, intellectual, religious, or political message is known as a hacktivist. Website defacement or denial-of-service assaults are typically at the heart of the most aggressive hacktivism.

IV. ETHICAL HACKING- TOOLS

4.1 NMAP

Network Mapper is referred to as Nmap. It is an open-source program used for network discovery and security audits. Although it was initially intended to scan huge networks, it can also be used to scan a single host. Network administrators also find it useful for activities like network inventory, scheduling service upgrades, and monitoring host or service uptime.

Nmap examines unprocessed IP packets to identify the network's available hosts. –

What hosts are there on the network, what services do they provide, what operating systems do they run on, what kind of firewalls do they employ, and other such fundamentals?

Nmap is compatible with several operating systems, including Windows, Mac OS X, and Linux.

4.2 Metasploit

One of the most effective exploit tools is Metasploit.

Most of its materials may be obtained at www.metasploit.com. It is a Rapid7 product. There are two versions of it: a paid edition and a free edition. It can be used with a web interface or a command prompt.

You may perform the following tasks using Metasploit:

- Carry out elementary penetration testing on small networks.
- To determine whether vulnerabilities can be exploited, conduct spot testing.
- To locate the network, import scan data.

It is possible to explore exploit modules and launch exploits on hosts.

4.3 Burp Suite

A well-known platform called Burp Suite is frequently used to do security testing on online applications. It provides a variety of tools that cooperate to assist the entire testing process, from initial mapping and monitoring of an application's attack surface through identification and exploitation of security flaws.

The administrators have complete control and can combine sophisticated manual procedures with automation for effective testing because of how simple it is to use. It is simple to set up and has features that will help even the most seasoned testers with their task. BurpSuite is designed to be an all-in-one toolkit, and BApps are add-ons that may be installed to expand its functionality.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

4.4 Angry IP Scanner

An easy-to-use, cross-platform IP address and port scanner is an angry IP scanner. Any IP address range can be scanned. You can use and copy it anywhere for free. It uses a multi-threaded strategy to speed up scanning, creating a separate scanning thread for each IP address being searched.

It merely pings each IP address to see if it is still active before resolving the hostname, figuring out the MAC address, scanning ports, etc. of each one. The quantity of obtained data or details about each host can be saved as IP-Port list files, TXT, XML, or CSV files. It may acquire any information about scanned IPs with the aid of plugins.

4.5 Ettercap

Ethernet Capture is referred to as Ettercap. This tool for network security can identify Man-in-the-Middle attacks. It features a variety of entertaining gimmicks, such as on-the-fly content screening and live connection sniffing. It contains tools for evaluating hosts and networks built in. Both actively and passively, many approaches can be examined.

Ettercap has various features for network and host analysis and enables both active and passive dissection of a wide range of protocols, including encrypted ones.

It is also possible to filter (substitute or drop a packet) on the fly and inject data into an established connection, maintaining connection synchronization. A robust and comprehensive sniffing suite is created with a variety of sniffing modes. IP-based, MAC-based, ARP-based (full-duplex), and Public ARP-based (half-duplex) are the four ways of sniffing that are available.

Ettercap can also identify switched LANs and determine the geometry of the LAN using OS fingerprints (active or passive).

4.6 Web Inspect

A tool for assessing the security of online applications called Web Inspect helps find both known and undiscovered vulnerabilities in the online application layer. Additionally, it might help in attempting common web attacks like parameter injection, cross-site scripting, directory traversal, and others, as well as making sure a Web server is configured properly.

4.7 LAN guard Network Security Scanner

The LAN guard Network Scanner keeps track of a network by scanning connected devices and reporting on each node. Every operating system has its information available.

The report can be set up in HTML format and it can also find registry problems. You may display information about each computer's Mac address, active user, and NetBIOS name table.

You can control and keep up end-point security across your network with LanGuard. It gives you visibility into every component of your network, allowing you to identify any potential vulnerabilities, and allows you to remedy those weaknesses.

4.8 LC4

LC4 was referred to as L0phtCrack. This is a program for auditing and recovering passwords. It is employed to evaluate the security of passwords and, in some circumstances, to recover forgotten passwords. By employing dictionary, brute force, and hybrid assaults, Microsoft Windows passwords can be cracked.

It recovers Windows user account passwords to simplify user transition to a different authentication method or to gain access to accounts with forgotten passwords.

4.9 Qualys Guard

A streamlined set of technologies called Qualys Guard can be used to cut expenses associated with compliance and streamline security operations. It automates the full range of IT system and web application audits, compliance, and protection, and it provides crucial security intelligence on demand. It includes a selection of tools for keeping track of, finding, and safeguarding your global network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

4.10 Ether Peek

For streamlining network analysis in a multiprotocol heterogeneous network environment, Ether Peek is an excellent tool. The installation process for Ether Peek takes only a few minutes and it is a small tool (less than 2 MB).
Packets of network communication are dynamically sniffed by Ether Peek. The default support includes AppleTalk, IP, NetWare, IP Address Resolution Protocol (ARP), TCP, UDP, NetBEUI, and NBT packets.

4.11 Network Stumbler

A Windows program called Network Stumbler scans and monitors WIFI. It makes WLANs detectable for network pros. Given that it aids in the identification of wireless networks that are not transmitting, networking hobbyists and hackers utilize it wisely.
It is possible to use it to check whether a network is configured correctly, to assess the network's signal strength or coverage, and to look for interference between one or more wireless networks. Moreover, it can be applied to establish connections with untrusted networks.

4.12 ToneLoc

Tone Locator is referred to as ToneLoc. In the early 1990s, a well-liked war dialing program was created for MS-DOS. A method known as "war dialing" entails using a modem to automatically call each phone number on a list of phone numbers, usually starting with the ones in the same area code. The created lists are used by malicious hackers to attack computer security, such as by figuring out user passwords or finding modems that could provide access to computers or other electronic systems. It can be used by security personnel to find unlawful devices on a business telephone network

V. PHASES OF HACKING

Phase 1: Reconnaissance

The stage of reconnaissance is where an attacker learns information about a target either actively or passively. Some of the instruments frequently used in this process include NMAP, Maltego, and Google Dorks.
There Are Two Types of Reconnaissance: Active and Passive: Through passive reconnaissance, information regarding the target is obtained without the targeted company's (or individual's) knowledge. It might be done easily by looking up information on the target on the internet or by paying off a worker at the targeted business to reveal and give the hacker useful information.
The term "information gathering" is also used to describe this process. In this method, the hacker doesn't attack the company's network or computer system to steal information.As opposed to passive reconnaissance, active reconnaissance involves the hacker entering the network to find specific hosts, IP addresses, and network services. It's also known as "rattling the doorknobs" when you do this. Compared to Passive Reconnaissance, there is a high risk of being caught when using this method.

Phase 2: Scanning

The attacker actively searches a target system or network during this phase for vulnerabilities that can be exploited. The tools used in this strategy are Nessus, Nexpose, and NMAP.
The data gathered in Phase 1 is used to examine the network in the scanning phase.To examine the network and gain access to the company's system and network, hackers use tools like dialers, port scanners, etc.

Phase 3: Gaining access

During this process, the vulnerability is found, and you try to exploit it to gain access to the machine. The main tool used in this procedure is Metasploit.
The hacker attacks and enters the local area network (LAN, either wired or wireless), local computer access, internet, or offline by using the information learned in the first two phases. It's Also Known As "Owning the System" in This Phase.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

Phase 4: Maintaining access

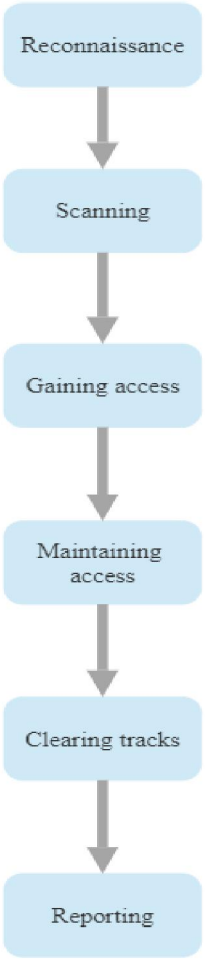
It is the technique a hacker uses to access a system. The hacker installs several backdoors after gaining access so that he can access the system again in the future if he needs to use this owned machine. The best tool for this method is Metasploit.

Phase 5: Clearing tracks

This practice is unethical. It has to do with clearing off any activity logs created throughout the hacking procedure.

Phase 6: Reporting

Reporting is the last stage of the ethical hacking process. Here, the ethical hacker compiles his results and the work that was accomplished, including the tools used, the rate of success, vulnerabilities found, and strategies used.



VI. COMMON HACKING TECHNIQUES

6.1 Phishing

The most popular hacking methods are phishing. Every day, phishing emails clog up all of our inboxes and text messaging program. These are messages that pose as either a company (such as Amazon, Netflix, etc.) or a person you trust and will, in most cases, fabricate a tale to trick you into opening an attachment or clicking on a link.

6.2 Bait and Switch Attack

Attackers may trick you into visiting harmful websites by using well-known marketing strategies like paid advertising on websites. Rogue attackers can purchase advertising space when websites sell it. A "bad" link that can be used to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

download malware, lock up your browser, or compromise your system infrastructure can take the place of a legitimate advertisement.
Alternatively, the advertisement may connect to a trustworthy website, but it will be set up to reroute you to a dangerous website.

6.3 Key Logger

A key logger is a little piece of software that records each keystroke when it is downloaded onto your computer. Every keystroke you make on the keyboard, together with your login, ID, password, credit card number, and other details, will be recorded by the key logger, revealing all your data and personal information.

6.4 Denial of Service (DoS\DDoS) Attack

A denial-of-service attack is a hacking technique intended to overload your web server with numerous requests, causing your website to break. To accomplish this, hackers will utilize zombie machines or botnets, with the sole purpose of saturating your website with data requests.

6.5 Clickjacking attacks

This technique tricks you into clicking on something other than what you intended to. A button on a web page that, when clicked, executes a separate function, and enables outsiders to take control of the device is an example of a clickjacking element. The host website may be unaware of the clickjacking detail.

6.6 Fake W.A.P

An imposter wireless access point (W.A.P.) can connect to the 'official' public place W.A.P. that you are using by utilizing software to mimic one. The moment you connect to the false W.A.P., a hacker has access to your data.
The hacker will give the false W.A.P. a name that appears to be legitimate, such as "T.F. Green Airport Free WIFI," to dupe you.

6.7 Cookie Theft

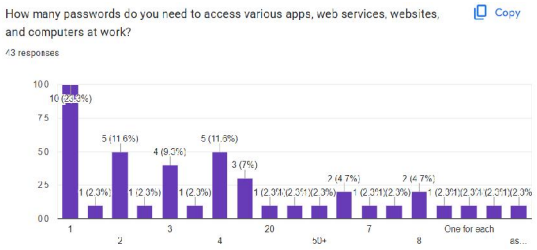
Our web browsers, such as Chrome, Mozilla, Safari, etc., utilize cookies to store personal information like our browsing history, usernames, and passwords for the numerous websites we visit. If the website you are visiting lacks an SSL (Secure Socket Layer) certificate, hackers can transmit data packets that travel through your computer.
In contrast to websites that start with HTTP:// (no 'S'), which lack SSL and are not regarded as secure, websites that begin with HTTPS:// are safe to visit.

6.8 Viruses and Trojans

When launched on a machine, viruses or Trojan horses are nefarious software packages that convey information from your machine to the hacker. Additionally, they can lock your data, spread it to every computer connected to your network, and perform a variety of other cruel deeds.
A Trojan Horse Virus is a form of malware that installs itself on a computer by impersonating a trustworthy application.

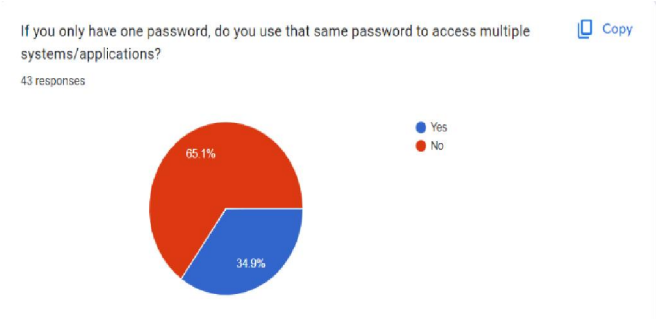
VII. RESEARCH METHODOLOGY

We conducted a survey where we asked a few questions to the people about how much they are aware of Ethical Hacking and what precautions they take to prevent it. The results are shown below:

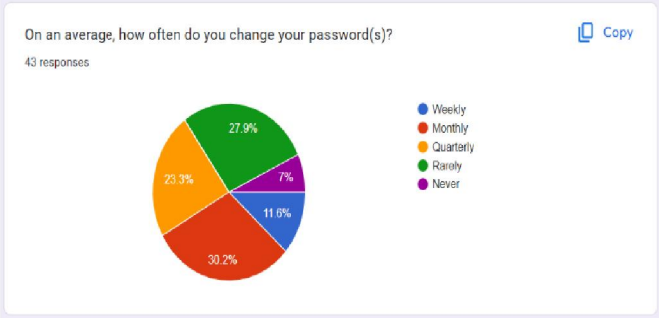


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

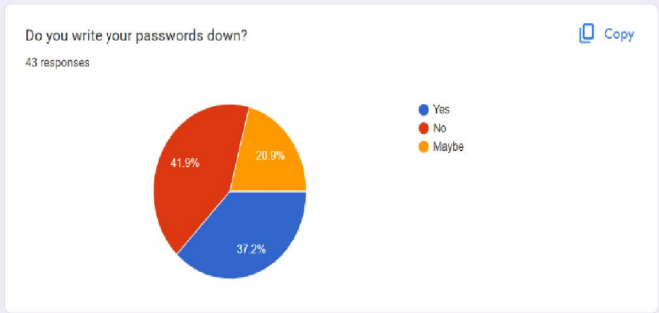
The above figure shows that many people keep the same password everywhere whether it be devices or websites or applications.



The above figure shows that very few people have a habit of keeping the password the same to access multiple applications/services.



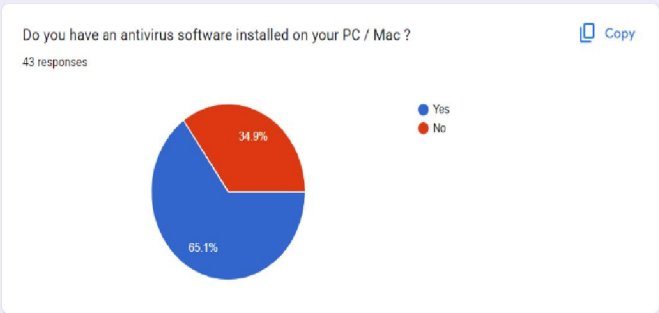
The analysis states that there is approximately an equal ratio of people changing their passwords monthly and rarely. There are very less people who never change their password ever.



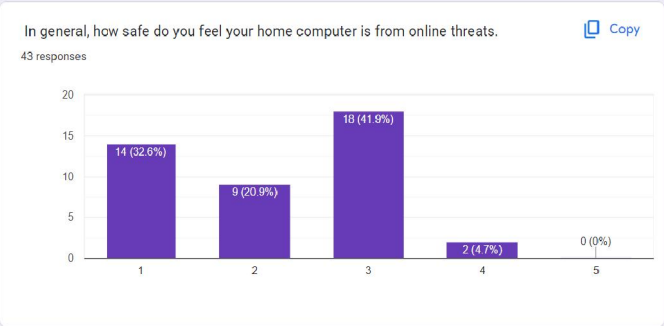
Here there is not much difference in the ratio of people writing down their passwords and not

When the respondents were asked about password protection or information security 63.5% strongly agreed, 33.3% agreed, and 3.3% were neutral bout this.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

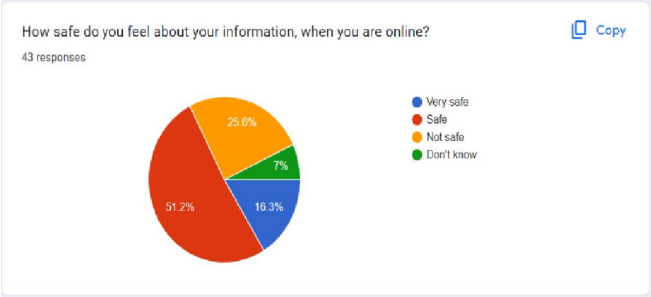


When the respondent was asked about that whether they have an antivirus installed on their devices then 65.1% of respondents answered "YES" and only 34.9 % answered "NO". This means that nowadays people are very well known about the threat of cybercrime.



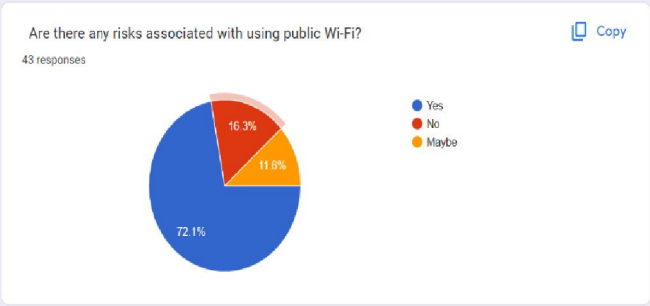
Out of 43 respondents, 41.9% are neutral about the security of their home computer from online threats, 32.6% feel the safest, 20.9% feel secure enough and 4.7% do not feel secure from online threats.

This question was all about checking the awareness of the respondent about cybercrime. In response to this question, 37.2% of the respondent were very well aware, 48.8% were aware of it, 14% were not well aware and only 0% of the respondents were not at all aware.

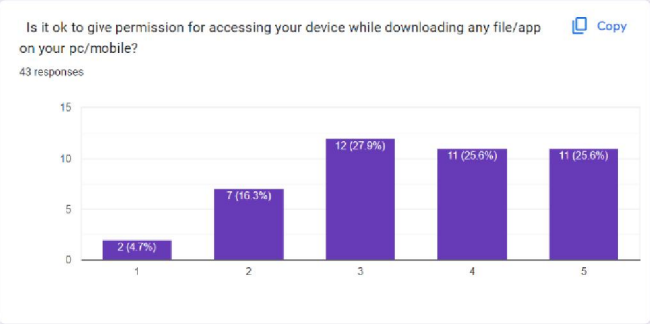


Of the respondent who answered this question as 16.3% think that online information is very safe, 51.2% think that is just safe, 25.6% agree on not safe and 7% were not know about the same.

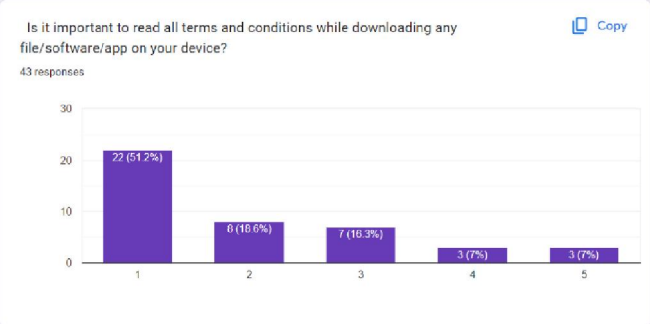
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023



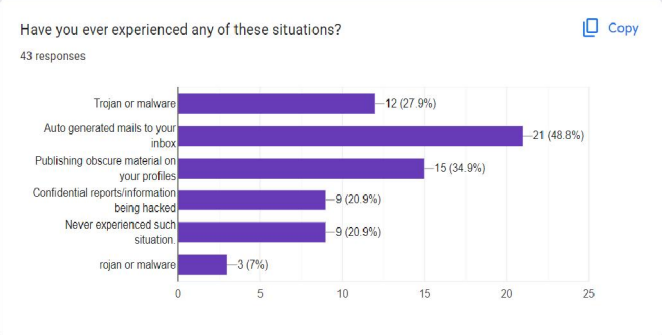
72.1% of the total respondents agree with the thought that there is a strong risk associated with the use of public Wi-Fi, 11.6% were neutral, and 16.3% disagree.



When this question was analyzed, the researcher finds that more than 80% of respondents were either neutral or disagree with it, and approx. 12% of respondents agreed with the same.



This is a very important factor for the online accessing of data, files, or information so 80% of the respondent agree on it or are neutral because when we download something from the internet, we should read all the terms and conditions before permitting access to our data.



Out of the 43 respondents, approximately 80% have experienced some or the other attack.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

According to the respondent, only 14% Strongly Agree with the effective cyber law to control crimes, the maximum population of the research was neutral (27.9%) while 11.6% of the total respondents strongly disagreed.

VIII. MEASURES TO BE TAKEN TO PROTECT YOUR SYSTEM FROM HACKERS

A. Install an anti-spyware package.

Software known as "spyware" is used to covertly track and collect private or business data. It frequently displays unsolicited advertisements or search results that are meant to direct you to particular (sometimes malicious) websites and is made to be difficult to identify and delete.

B. Install antivirus software.

By spotting potential attacks in real-time and protecting your data, antivirus software is crucial to keeping your system secure. Automatic updates are a feature of several robust antivirus programs that further shield your computer from the daily crop of new dangers. After installation, don't forget to use your antivirus program. Run or schedule routine virus scans to keep your machine clear of malware.

C. Use virtualization

There is no requirement for everyone to choose this route, but if you do, be prepared to encounter spyware and viruses. While staying away from risky websites is the best defense against browser-related intrusions, virtualization enables you to use your browser in a protected virtual environment that works independently of your operating system, such as Parallels or VMware Fusion.

D. Use complex passwords

Using secure passwords is the most critical approach for preventing network attacks. The more secure your passwords, the more difficult it will be for a hacker to gain access to your system. More secure typically means longer and more complicated. Use a password that is at least eight characters long and consists of a combination of numbers, uppercase and lowercase letters, and computer symbols. Hackers may hack short, easy passwords in minutes using a variety of techniques.

E. Secure your network

Routers are rarely provided with the highest security settings activated. While configuring your network, log in to the router and set a password using a secure, encrypted setup. This prevents intruders from breaking into your network and messing with your configuration.

F. Use encryption

Even if hackers gain access to your network and files, encryption can keep them from gaining access to your data. You can encrypt your Windows or macOS hard drive using BitLocker (Windows) or FileVault (Mac), as well as any USB flash drive containing sensitive data and online traffic with a VPN. Only shop on encrypted websites, as indicated by the "https" in the address bar, which is accompanied by an image of a closed padlock.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

X. CONCLUSION

The practice of ethical hacking should no longer be viewed as criminal conduct since it is not one. Hacking that is detrimental is illegal and against the law, but ethical hacking is never wrong. Ethical hacking complies with organizational IT policy as well as industry norms.

While malicious hacking should be avoided, ethical hacking that advances study, invention, and technological advances should be encouraged and permitted

REFERENCES

[1] Conrad J. (2012). Seeking help: The important role of ethical hackers. Network Security. 2012(8), pp.5-8. doi:10.1016/s1353- 4858(12)

[2] Sukhai, N.B. (2004). Hacking and cybercrime.InfoSecCD Proceedings of the 1st annual conference on Information security curriculum development, ACM. pp. 128-132.

[3] Farwell J.P., Rohozinski R. (2011). Stuxnet and the future of cyber war. Survival.

[4] Machin, S. and Meghir, C. (2004). Crime and economic incentives. Journal of Human Resources, 39(4), pp.958-979.

[5] Fehr C., Licalzi C., Oates T. (2016). Computer crimes. The American Criminal Law Review, 53(4)

[6] https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_quick_guide.htm

[7] https://en.kali.tools/?p=107

[8] Elsevier B.V (2002). In Argentina, a judge ruled that hacking is not a crime, Computer Fraud & Security, 2002(5), p.20.

[9] https://hack4net.github.io/Hacking-Tutorial/