

# BLOB

VOLUME 03 | ISSUE 01 | May 2022



# CYBER SECURITY

**DEPARTMENT OF  
COMPUTER SCIENCE  
AND ENGINEERING**

MEA Engineering College,  
Perinthalmanna





# Department of Computer Science & Engineering

## Vision

The Computer Science and Engineering department is committed to provide an educational environment in order to develop professionals with strong technical skills and aptitude towards the research and entrepreneurship.

## Mission

- To impart quality education to the aspiring students for improving their level of confidence to solve various engineering problems.
- To deliver a perfect blend of technical and soft skills for creating competent computer engineers with professional and ethical values.
- To cultivate an environment of intellectual growth in pursuit of academic and research activities.



# Editorial Board

Chief Editor : Dr. Raji C G

Managing Editor : Ms. Rashida Farsath K

Editorial Board Members: Mr. Jemsheer Ahmed P  
: Ms. Najla Musthafa  
: Mr. Mohammed Aseel  
: Ms. Fathima Rishana P P  
: Ms. Hannathu Nishana P A  
: Ms. Hajira Shuhaila

Design Team : Mr. Asheeq Akthar C  
: Mr. Mufleh Mohamed P  
: Mr. Muhammed Muhsin P  
: Mr. Muhammed Dishan V

## Editorial

Welcome to the fourth edition of "Blob", the magazine that explores the latest trends and developments in technology. In this edition, we focus on Cyber Security and its relevance in the modern world.

The importance of Cyber Security cannot be overstated, as cyber threats are becoming more sophisticated and prevalent in our increasingly digital world. In this edition, we delve into the topic of Cyber Security and how it affects our daily lives, both at home and in the workplace.

We have a range of expert contributors who provide insights into the latest cyber threats and how they can be mitigated. Our contributors discuss a variety of topics, such as the impact of social engineering attacks, the rise of ransomware, and how to secure cloud-based systems

We believe that this edition of "Blob" will be a valuable resource for anyone who wants to stay up-to-date with the latest developments in Cyber Security. Whether you are a business owner, an IT professional, or simply someone who is interested in the topic, you will find something of interest in this edition.

We hope you enjoy reading "Blob" and gain valuable insights from our contributors. We welcome your feedback and suggestions for future editions. Thank you for your continued support, and we hope you enjoy reading the latest edition of "Blob."

“The  
Internet is  
becoming  
the town  
square for  
the global  
village of  
tomorrow”  
– Bill Gates



Mr. Jemsheer Ahmed P  
Editorial Board Member



# CRYPTO-CURRENCY HEIST



**Mohammed Shameel P**  
MEA19CS051

## Introduction

Cryptocurrency and Crime examine well-known incidents of cybercrime involving the theft (or otherwise illegal acquisition) of cryptocurrency, as well as some of the methods and security flaws typically exploited. Cryptojacking is a type of cybercrime that has been utilized on websites to take over a victim's resources and use them for hashing and mining cryptocurrency. Illicit activities such as cybercrime, money laundering, and



terrorism financing accounted for only 0.15 percent of all crypto transactions in 2021, totaling \$14 billion, according to blockchain analysis firm Chainalysis.

Blockchain is the technology that enables the existence of cryptocurrency (among other things). Bitcoin is the name of the best-known cryptocurrency, the one for which blockchain technology was invented.



### Technology Used

1. **Cryptocurrency exchanges:** These are platforms that allow users to buy, sell, and store cryptocurrencies. A vulnerability in the security of exchange can lead to the loss of large amounts of cryptocurrency.
2. **Wallets:** Digital wallets are used to store cryptocurrencies and can be vulnerable to hacking if not properly secured.
3. **Decentralized finance (DeFi) protocols:** DeFi protocols are built on blockchain

technology and allow users to carry out financial transactions without the need for intermediaries. However, they can also be vulnerable to attacks if their smart contract code contains vulnerabilities.

4. **Phishing scams:** Phishing scams are a common way for hackers to steal cryptocurrencies. They often involve the use of emails, messages, or websites that look like they're from a legitimate source but are designed to steal sensitive information such as private keys.
5. **Malware:** Malware is a type of software that is designed to harm a computer or steal information. In the context of cryptocurrency, malware can be used to steal private keys and access funds stored in a wallet.

### Tools Used In Cryptocurrency Heists

The tools used in cryptocurrency heists can vary depending on the specific type of attack. However, here are some common tools that are used in such attacks:

- **Malware:** Malware is a type of software that is designed to harm a computer or steal information. In the context of cryptocurrency, malware can be used to steal private keys and access funds stored in a wallet.
- **Phishing kits:** Phishing kits are pre-made templates and tools that are used to carry out phishing attacks. They are designed to make it easier for attackers to create fake websites or emails that look like they're from a legitimate source.
- **Exploit kits:** Exploit kits are collections of software vulnerabilities that are packaged together for use by attackers. They can be



used to exploit vulnerabilities in software and gain unauthorized access to systems.

- **Remote access Trojans (RATs):** RATs are a type of malware that allows attackers to remotely control an infected computer. In the context of cryptocurrency, RATs can be used to steal private keys and access funds stored in a wallet.
- **Cryptojacking software:** Cryptojacking software is a type of malware that uses an infected computer's resources to mine cryptocurrency without the owner's consent. This type of software can also be used to steal private keys and access funds stored in a wallet.

These are just a few examples of the tools that are used in cryptocurrency heists. To prevent such attacks, it's important to use strong passwords, enable two-factor authentication, store private keys offline, and be cautious of phishing scams and suspicious emails or messages.

### Ways To Protect Yourself From Cryptocurrency Heists

- **Use strong and unique passwords:** Use strong and unique passwords for all of your online accounts, including your cryptocurrency wallets and exchanges.
- **Enable two-factor authentication (2FA):** Enable two-factor authentication (2FA) wherever possible to add an extra layer of security to your accounts.
- **Store private keys offline:** Store your private keys offline, on a hardware wallet or a piece of paper, to reduce the risk of them being stolen.
- **Be cautious of phishing scams:** Be cautious of phishing scams and suspicious



emails or messages, and never reveal your private keys or other sensitive information to anyone.

- **Use reputable exchanges and wallets:** Use reputable exchanges and wallets that have a good track record for security.
- **Keep your software up-to-date:** Make sure to keep your software, including your operating system and any security software, up-to-date to protect against known vulnerabilities.
- **Diversify your investments:** Diversify your investments across different types of cryptocurrencies and different wallets to reduce the risk of losing everything in the event of a hack.

## Conclusions

Cryptocurrency heists are a growing threat in the digital world and individuals and organizations need to take steps to protect themselves. Cryptocurrency heists can take many forms, including phishing scams, malware, exchange hacks, wallet hacks, social engineering, and 51% attacks. These attacks can result in the loss of large amounts of cryptocurrency.

However, there are several simple steps you can take to protect yourself from cryptocurrency heists, including using strong and unique passwords, enabling two-factor authentication, storing private keys offline, being cautious of phishing scams, using reputable exchanges and wallets, keeping your software up-to-date, and diversifying your investments. By following these steps, you can reduce the risk of having your cryptocurrencies stolen and keep your investments safe.



# ATTACKS ON THE HEALTH- CARE SECTOR

---



**Fathima Nidha PK**  
MEA19CS019

## Introduction

The cyberthreat to the healthcare business has grown significantly, as has the sophistication of cyberattacks. Both business and government understand this new age. With each advancement in automation, interoperability, and data analytics, the susceptibility to hostile intrusions grows. Attacks on the healthcare sector can have serious consequences such as financial losses, theft of personal information, disruption of



crucial medical services, and harm to patient health. Healthcare organizations are often targeted because they store sensitive and valuable information. Cyberattacks are of special concern in the health industry because they can endanger not just the security of systems and information, but also the health and safety of people.

For three key reasons, healthcare businesses are appealing targets for cybercriminals:



- Criminals can swiftly sell patient medical and billing information on the darknet for insurance fraud reasons.
- The capacity of ransomware to lock down health care and back-office systems makes large ransom payments possible.
- Medical gadgets that are connected to the internet are vulnerable to manipulation.

## Types of Attacks on the Healthcare Sector

The healthcare sector is vulnerable to various forms of attack, including:

### 1. Ransomware:

This type of attack encrypts data and demands payment for the decryption key. Ransomware attacks, where malware encrypts important data and demands payment for the decryption key, are a common type of attack on the healthcare sector. The sector is particularly vulnerable because they cannot afford prolonged system downtime and may therefore pay the ransom.

### 2. Phishing:

Phishing attacks, where attackers send emails or messages appearing to be from a trustworthy source, are also becoming increasingly common. Insider threats, where employees with access to sensitive information abuse their privileges, are also a concern.

### 3. Insider Threats:

These attacks are performed by individuals who have authorized access to the systems and data of a healthcare organization, but use it for malicious purposes.

### 4. Malware:

This involves infecting computers or networks with harmful software that can steal information or interrupt operations.

### 5. DDoS:

This type of attack inundates a healthcare organization's systems with excessive traffic, making it difficult for legitimate users to access their services.

### 6. Supply Chain Attacks:

This involves compromising the security of third-party vendors that supply healthcare organizations with products or services.

### 7. Medical Device Attacks:



This type of attack targets medical devices connected to the internet, which can be easily hacked.

It is crucial for healthcare organizations to be aware of these threats and take necessary security measures, such as regular software updates, staff cybersecurity training, and utilizing encryption and firewalls to secure sensitive data.

**Impacts in the attack on the Healthcare sector**

The attack on the healthcare industry has the potential to have a wide-ranging impact. Among these effects are the following:

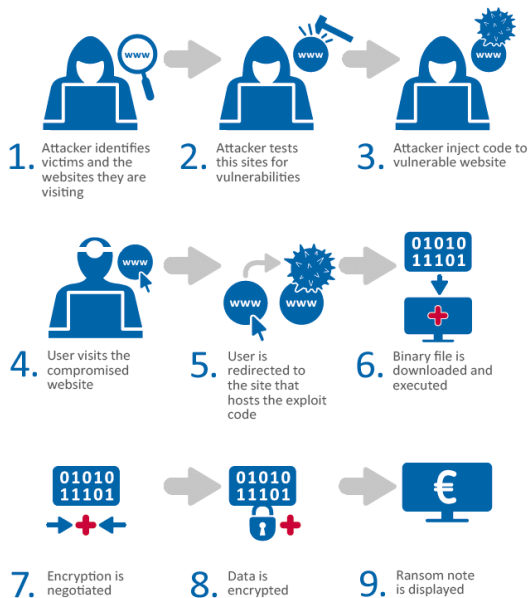
- Patient care disruption: Healthcare organisations are responsible for providing important services to patients, and any disturbance in their operations can cause injury or delay in treatment.
- Personal health information (PHI) at a healthcare business is a desirable target for attackers, who can exploit it for identity

- theft, fraud, or other malevolent objectives.
- Financial loss: Healthcare companies may face large financial losses as a result of the expenses of restoring systems and repairing damage, as well as possible revenue loss due to service disruption.
- Damage to a healthcare organization’s reputation: An assault on a healthcare institution can harm its reputation and diminish faith in its capacity to secure patient information and deliver excellent care.
- Issues with compliance: Healthcare firms are subject to stringent rules governing patient data protection and privacy, and a data breach can result in substantial fines and penalties.

Because the effects of a successful assault can be far-reaching and long-lasting, healthcare institutions must take proactive efforts to defend their systems and prevent attacks.

The attack on the healthcare industry can result in several important consequences. These can include disruptions in patient care, the loss of confidential patient information, financial losses, harm to the organization’s reputation, and potential non-compliance with regulations. To minimize the risk of such an attack, healthcare organizations need to take proactive steps to secure their systems and protect sensitive data.

ATTACK SCENARIO 4 – RANSOMWARE



**Preventive Measures**

To prevent attacks on the healthcare sector, the following steps can be taken:

1. Employee training: Healthcare organizations should train their staff on cyber threats, including phishing and



ransomware.

2. Strong passwords: A strong password policy, requiring unique and complex passwords, can prevent unauthorized access to sensitive information.
3. Network defense: Implementing security measures such as firewalls and intrusion detection can protect healthcare networks and systems.
4. Data protection: Encrypting sensitive data like medical records can safeguard it from theft and unauthorized access.
5. Software updates: Keeping software up-to-date with the latest security updates can prevent vulnerabilities from being exploited.
6. Backup and recovery: Regular data backups and a disaster recovery plan can help organizations recover from a cyber attack or data loss.
7. Third-party management: Careful vetting and monitoring of third-party vendors, including cloud-based service providers, is necessary to reduce risk.
8. Security evaluations: Regular security evaluations, such as penetration testing and vulnerability scanning, can identify and address security weaknesses before they are exploited by attackers.

## Conclusion

In conclusion, the healthcare industry is under attack, and healthcare organizations must take proactive actions to safeguard themselves and their patients. Healthcare businesses may lower the chance of a successful attack and lessen the effects if one occurs by installing robust security measures and routinely training personnel on security best practices.



# CONTINUED RISE IN RANSOM- WARE

---



**Khadeeja Shehin CK**  
MEA19CS033

## Introduction

Ransomware is a malicious software that locks a victim's files, making them inaccessible until a ransom is paid. It poses a major threat to businesses, individuals, and governments and can cause substantial financial and operational damage. With the growing use of digital devices and the increasing sophistication of attackers, ransomware attacks are becoming more prevalent. The purpose of ransomware is to extract money from the victim, with the



ransom usually demanded in cryptocurrency for its anonymous nature. The consequences of a ransomware attack can be serious, so it's crucial for people and organizations to take necessary measures to secure their systems and data, such as using strong passwords and backing up important information regularly.

## Factors Contributing To The Rise Of Ransomware Attacks

Several factors are leading to the rise in



ransomware attacks, including

1. Widespread use of digital devices: The increasing use of computers, smartphones, and cloud systems has created a large number of potential targets for ransomware attacks.
2. Growing reliance on cloud systems: The use of cloud-based systems to store data has made it easier for attackers to launch ransomware attacks.
3. Increased use of cryptocurrency: The

growing adoption of cryptocurrencies, such as Bitcoin, as a payment method for ransoms has made it easier for attackers to receive payments anonymously.

4. Attacker sophistication: Ransomware attacks are becoming more sophisticated as attackers gain access to advanced tools and techniques.
5. Expansion of the dark web: The dark web provides a platform for ransomware groups to operate and sell and trade malware and tools.
6. Inadequate security measures: Many individuals and organizations are not taking the necessary steps to protect their systems and data, making them more vulnerable to ransomware attacks.
7. Human error: Social engineering tactics, such as phishing emails, can trick individuals into downloading and installing ransomware, making human error a common cause of ransomware infections.

These factors are contributing to the continued increase in ransomware attacks and their growing impact. It is crucial for people and organizations to be aware of these factors and take measures to protect themselves from ransomware attacks.

### **Recent Ransomware Attacks**

Recently, there have been several high-profile cases of ransomware attacks, including:

1. Colonial Pipeline attack: The Colonial Pipeline was targeted by a ransomware attack in May 2021, which led to a widespread fuel shortage across the United States. The company was forced to pay a ransom of \$4.4 million to the



attackers.

2. JBS USA attack: In June 2021, the largest meat processing company in the world, JBS USA, was hit by a ransomware attack that resulted in major disruptions to its operations. The company later confirmed that it had paid the ransom to the attackers.
3. Ireland's Health Service Executive breach: In April 2021, the Irish Health Service Executive fell victim to a ransomware attack that caused the loss of sensitive information. The attackers demanded a ransom of \$20 million.
4. LG Electronics attack: In November 2021, LG Electronics was impacted by a ransomware attack that affected its operations in several countries. The attackers demanded a ransom of \$10 million.
5. Ransomware attacks on schools: In recent years, there has been a rise in ransomware attacks targeting schools and universities. These attacks often result in the loss of sensitive data and disruptions to their operations.

These are only a few examples of the numerous ransomware attacks that have taken place in recent years. The prevalence and severity of these attacks emphasize the need for individuals and organizations to take measures to protect against ransomware.

## **Protection From Ransomware Attacks**

To defend against ransomware attacks, individuals and companies can take the following steps:

1. Regular backup: Backing up critical data and storing it securely is a crucial step in protecting against ransomware. This way, if an attack occurs, the data can be restored without having to pay a ransom.
2. Software updates: Keeping all software, including operating systems and applications, up to date and patched can prevent vulnerabilities that ransomware attackers might exploit.
3. Strong passwords: Implementing strong, unique passwords and changing them frequently is an effective way to defend against ransomware and other cyber attacks.
4. Employee training: Educating employees on the dangers of ransomware, how to identify phishing emails, and how to handle suspicious links or attachments can minimize the risk of a ransomware attack.
5. Two-factor authentication: Implementing two-factor authentication can prevent unauthorized access to systems and data, even if a password is compromised.
6. Antivirus and anti-malware software: Installing and updating antivirus and anti-



malware software can detect and prevent ransomware attacks.

7. Restricted access: Limiting access to sensitive data and systems to only those who need it can decrease the risk of a successful ransomware attack.

By taking these and other protective measures against ransomware, individuals and organizations can decrease their risk of being attacked and minimize the impact if an attack occurs.

## Conclusion

To summarize, the ongoing increase in ransomware attacks is a major problem that

affects everyone. The use of digital devices, cloud systems, and cryptocurrencies, along with the growing sophistication of attackers, make it easier for them to carry out these attacks. The consequences can be devastating, causing significant financial and operational damage. Taking preventive measures, such as backing up data, using secure passwords, and educating employees, can help reduce the risk of a successful attack and minimize its impact. The continued rise in ransomware attacks emphasizes the importance of being proactive about cyber security and taking necessary measures to protect against these attacks.



# SECURITY IN CLOUD COMPUTING



**Abhishek KP**  
LMEA19CS096

## Introduction

Cloud computing is not a new technology; rather, it is a new method of distributing information and services utilizing current technologies. It utilizes the network architecture of the internet to link client-side and server-side services and applications (Weiss, 2007). Similar to how internet service providers offer high-speed broadband for customers to access the internet, cloud service providers (CSPs) offer cloud platforms for their



clients to use and develop web services. CSPs and ISPs both offer services. The cloud adds a layer of abstraction between the involved low-level architecture and processing resources. Customers pay a membership fee to the cloud service provider, who then grants them access to the cloud's resources and physical infrastructure. Customers do not control the actual infrastructure. Because they can purchase anything from the cloud services provider, customers can save money on





resources like hardware, licencing, and other services (like email). Recent surveys show that embracing cloud computing allowed disciplined firms to save an average of 18% on their IT budget and 16% on data center electricity costs (McFedries, 2008). The most significant cloud computing components are outlined in this study.

### Cloud Architecture

The following are five essential characteristics

of cloud computing that give it an edge over similar technologies:

- Unlike past computing models, cloud computing is based on a business model in which resources are shared at the network, host, and application levels. This is known as multitenancy (shared resources)..
- Huge scalability: With cloud computing, you may scale up to tens of thousands of devices and significantly increase bandwidth and storage capacity.
- Massive scalability: With cloud computing, you may scale to tens of thousands of systems and significantly increase bandwidth and storage capacity.
- Pay-as-you-go:Users only pay for the resources they actually use and for the time that they actually utilize them.
- Self-provisioning of resources: Users can self-provision new systems and network resources (processing power, software, and storage).

### Cloud Deployment Models

Public, private, and hybrid clouds are the three basic types of cloud deployment models.

- **Public cloud** - The most common type of cloud is this one. Here, a number of users can connect to the internet to access web services and apps. Each customer has unique resources that are dynamically provisioned by a third-party provider. This third-party provider maintains all security, hosts the cloud for numerous customers across numerous data centres, and supplies the necessary hardware and infrastructure for the cloud to function. The customer has no influence over, knowledge of, or access to the infrastructure that makes up



the cloud.

- **Private Clouds** - A personal network that mimics the idea of the cloud. They allow users to take advantage of cloud computing's advantages while avoiding some of its downsides. You have total control over data management and security with private clouds. This can make users feel more assured and in control. This deployment option's main drawback is that users will incur high expenses because they will have to pay for cloud infrastructure and manage the cloud themselves.
- **Hybrid Clouds** - These networks integrate private and public clouds. It enables companies to benefit from both deployment models. For instance, a business could store sensitive information on its private cloud and use the public cloud to address circumstances with high traffic and demand.

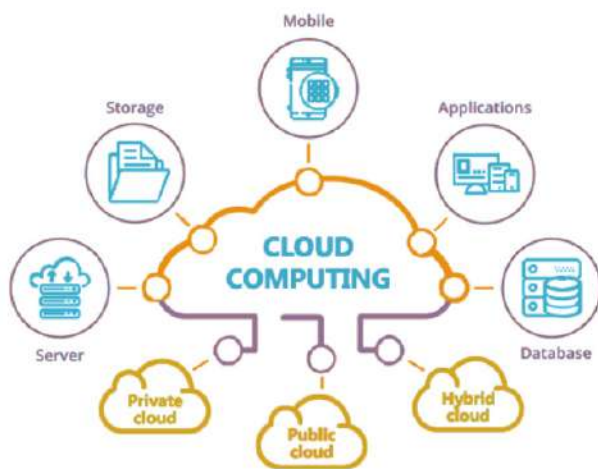
### **Cloud Computing**

What steps make up the cloud computing process? What does using the cloud mean for your computer use? What apps for cloud computing are the most widely used? All of them are valid inquiries, and this study on cloud computing provides answers to each one. That will transform how you work and collaborate online. While I do try to give you a thorough overview of the cloud computing phenomenon and introduce you to some of the more well-known cloud applications, especially those that support group collaboration, I do not make any claims to be able to answer all of your questions (especially the more technical ones) And here is where cloud computing



really excels. Cloud computing may facilitate communication and collaboration amongst group members whether you're trying to manage a multidimensional project in a huge corporation, organise volunteers for a community organisation, or share photos with family members. If you read the book, you'll understand how this works better, but if you need to cooperate, cloud computing is the way to go. Google lists the following six essential traits of cloud computing:

1. The user comes first with cloud



computing. Everything that is kept on the cloud—documents, messages, photos, programmes, and so forth—becomes yours the moment you connect to it. Additionally, you can share the data with others and it is not only yours. Any gadget that uses your cloud data effectively becomes yours as well.

2. Cloud computing focuses on tasks. Instead of concentrating on the programme and what it can do, think about what you need to get done and how the application can assist you do it. Email, spreadsheets, word processing, and other conventional tools

are becoming less important than the material they produce.

3. Powerful cloud computing exists. A vast amount of computing power is produced by joining hundreds or thousands of computers in a cloud, which is not achievable with a single desktop PC. It is possible to use cloud computing. Users can rapidly obtain more information from many sources because data is kept in the cloud. Unlike with a desktop PC, you are not constrained to a single data source.

4. Cloud computing is a smart technology. Data mining and analysis are required to access the variety of data that is stored on the computers in a cloud in an intelligent way.

5. Cloud computing is adaptable. Many of the tasks required by cloud computing must be automated. Information saved on a single cloud computer, for instance, must be replicated on additional cloud computers to protect the integrity of the data. The cloud's algorithm redistributes the data from that machine to another cloud computer if that one goes offline.

## Why Computing Advantage and Dis-advantage

### Advantage as below,

1. Lower-Cost Computers for Users
2. Improved Performance
3. Lower IT Infrastructure Costs
4. Fewer Maintenance Issues
5. Lower Software Costs
6. Instant Software Updates
7. Increased Computing Power
8. Unlimited Storage Capacity
9. Increased Data Safety
10. Improved Compatibility Between

## Operating Systems

11. Improved Document Format Compatibility
12. Easier Group Collaboration
13. Universal Access to Documents
14. Latest Version Availability
15. Removes the Tether to Specific Devices

## Disadvantage as below,

1. Requires a Constant Internet Connection
2. Doesn't Work Well with Low-Speed Connections
3. Can Be Slow
4. Features Might Be Limited
5. Stored Data Might Not Be Secure
6. If the Cloud Loses Your Data, You're Screwed

## Conclusion

One of the primary security issues with the cloud computing idea is the sharing of resources (multitenancy). The security level offered by cloud service providers must be disclosed to their present clients. The advantages and disadvantages of various

cloud deployment models, such as public, private, and hybrid clouds, must be explained to prospective clients by cloud service providers. They must show their customers that they are taking the required security precautions to protect their data and foster confidence in their business. Companies can achieve this by using third-party auditors (Mikkilineni & Sarathy, 2009). New security methods must be created, and current security tactics must be radically changed in order to work with the cloud architecture. Plugging in current security devices won't work since this new delivery model requires fundamental changes to how we access and use computer resources. New security methods must be created, and current security tactics must be significantly modified in order to work with the cloud architecture. Plugging in current security devices will not work since this new delivery model requires fundamental changes to how we access and use computer resources.



# SECURITY FOR MOBILE PLATFORMS

---



**Mohammed Aflah**  
MEA21CS037

## Introduction

Mobile security is the protection of smartphones, tablets, and laptops from threats associated with wireless computing. Mobile devices like laptops, tablets, and smartphones with desktop-computer capabilities are the future of computing and communication. They are excellent for usage from anywhere with an internet connection because of their size, operating systems, applications, and computing power. With





the rise of ruggedized devices, the Internet of Things (IoT), and operating systems like Chrome OS, macOS, and Windows 10, any piece of hardware with these characteristics becomes a mobile computing device.

Organizations and users have decided to buy and use mobile devices over desktop computers because they have grown more affordable and portable. And, as wireless internet connection becomes more widespread, all types of mobile devices are becoming more vulnerable to attacks and data breaches.

Authentication and authorisation across mobile devices is convenient, but it increases risk by removing the limits of a secure organisational boundary. Multi-touch

displays, gyroscopes, accelerometers, GPS, microphones, multi-megapixel cameras, and ports, for example, expand a smartphone's capabilities and enable for the attachment of more devices. These new features alter how users are verified and authorization is distributed locally to devices, apps, and services on a network. As a result of the additional capabilities, the number of endpoints that require cybersecurity protection is expanding.

Cybercriminals can now hack into cars, security cameras, baby monitors, and medical implants. By 2025, there might be over 75 billion "things" connected to the internet, including cameras, thermostats, door locks, smart TVs, health monitors, and other devices.

While establishing and enforcing an enterprise-wide security policy is vital, it isn't enough to combat the volume and variety of today's mobile threats. In 2019, Verizon conducted a poll of 670 security professionals with prominent mobile security businesses, including IBM, Lookout, and Wandera . According to the study, one out of every three people surveyed had experienced a mobile device compromise. Remediation was "complex and expensive" for 47% of respondents, while 64% experienced downtime.

Companies that encourage employees to bring their own devices (BYOD) face increased security threats. They provide potentially untrusted devices access to company servers and critical datasets, making them vulnerable to attack. Cybercriminals and fraudsters can take advantage of these flaws to injure or damage the person and the company. They're



looking for trade secrets, insider information, and unlawful access to a secure network in order to locate anything lucrative.

## **Mobile security threats**

### **Phishing**

Phishing is a fraudulent effort to steal users' credentials or sensitive data, such as credit card details, and is the most common mobile security concern.

### **Malware and Ransomware**

Mobile malware is undetectable software that is designed to harm, disrupt, or obtain unauthorized access to a client, computer, server, or computer network. Ransomware is a type of virus that threatens to delete or lock down a victim's data or files unless a ransom is paid to unlock the files and restore access.

### **Cryptojacking**

Cryptojacking is a type of malware that mines cryptocurrencies like Bitcoin and Ethereum using an organization's or individual's computing capacity without their knowledge, reducing a device's processing powers and efficacy.

### **Unsecured wifi**

Mobile devices are more exposed to cyberattacks while using unsecured wifi hotspots without a virtual private network (VPN). Cybercriminals can use Man-in-the-middle (MitM) attacks to eavesdrop on network traffic and obtain sensitive personal data. Users can also be duped into connecting to rogue hotspots, making it easier for cybercriminals to harvest business or personal data.

### **Outdated operating systems**

Exploiting vulnerabilities in outdated operating systems (OSs) has been a common tactic for cybercriminals. Devices that run on old OSs are still susceptible to attacks, and security patches are often included in manufacturer updates to address active vulnerabilities.

### **How to secure mobile devices**

Mobile devices and non-mobile PCs have the same basic security needs. In general, secrecy, integrity, identity, and non-repudiation must all be maintained and protected. Today's mobile security developments, on the other hand, provide new difficulties and opportunities, necessitating a rethinking of personal computing device security. Device form factor (size and shape), developments in security technology, continuously expanding attack strategies, and device interface, such as touch, audio, and video, all affect capabilities and expectations.

Because of device capabilities, the mobile threat landscape, and evolving user expectations, IT companies and security teams must reassess how to meet security needs. In other words, these experts must protect various vulnerabilities in a constantly changing and rapidly expanding mobile device environment. Enterprise mobility management, email security, endpoint protection, VPN, secure gateways, and cloud access broker are all areas in which a secure mobile environment will provide protection.

Cybercriminals are becoming more determined and sophisticated, resulting in more damaging, multi-faceted hacks that

are more difficult to detect, necessitating increased security and vigilance. The purpose of this report is to help consumers understand the risks they face and learn how to stay safe while computing on all of their devices.

Cybercriminals mostly employ risky apps to transmit malicious malware, hacking tools, and connections to hacked websites. Cyber thieves can infect a user's mobile device by downloading malicious malware aimed to steal personal information or carry out any other fraud scheme using dangerous applications.

As we'll see in a moment, phishing on mobile is on the rise, thanks to the proliferation of dangerous applications that have infected URLs that link to sites with drive-by downloads, and roughly 25% of risky apps that contain malware also contain suspicious URLs.

Cybercriminals use mobile environments

to monetize through special underground partnership programmes, the main idea of which is to distribute malicious code on a wide range of smartphones based on popular OS's through landing pages or mobile traffic (iOS, Windows Mobile, Google Android, and so on), and then ask for paid SMS or do it silently on specially crafted paid numbers from grey SMS billings providers.

## Conclusion

A non-malware approach is essential for securing mobile devices, as data-leaking apps pose a more significant threat than traditional malware. Even applications downloaded from certified app stores can have serious security vulnerabilities. Effective mobile security requires identifying and resolving security weaknesses in device operating systems, configurations, and network connections used by apps on a regular basis.





# OPEN SOURCE TOOLS FOR CYBER SECURITY

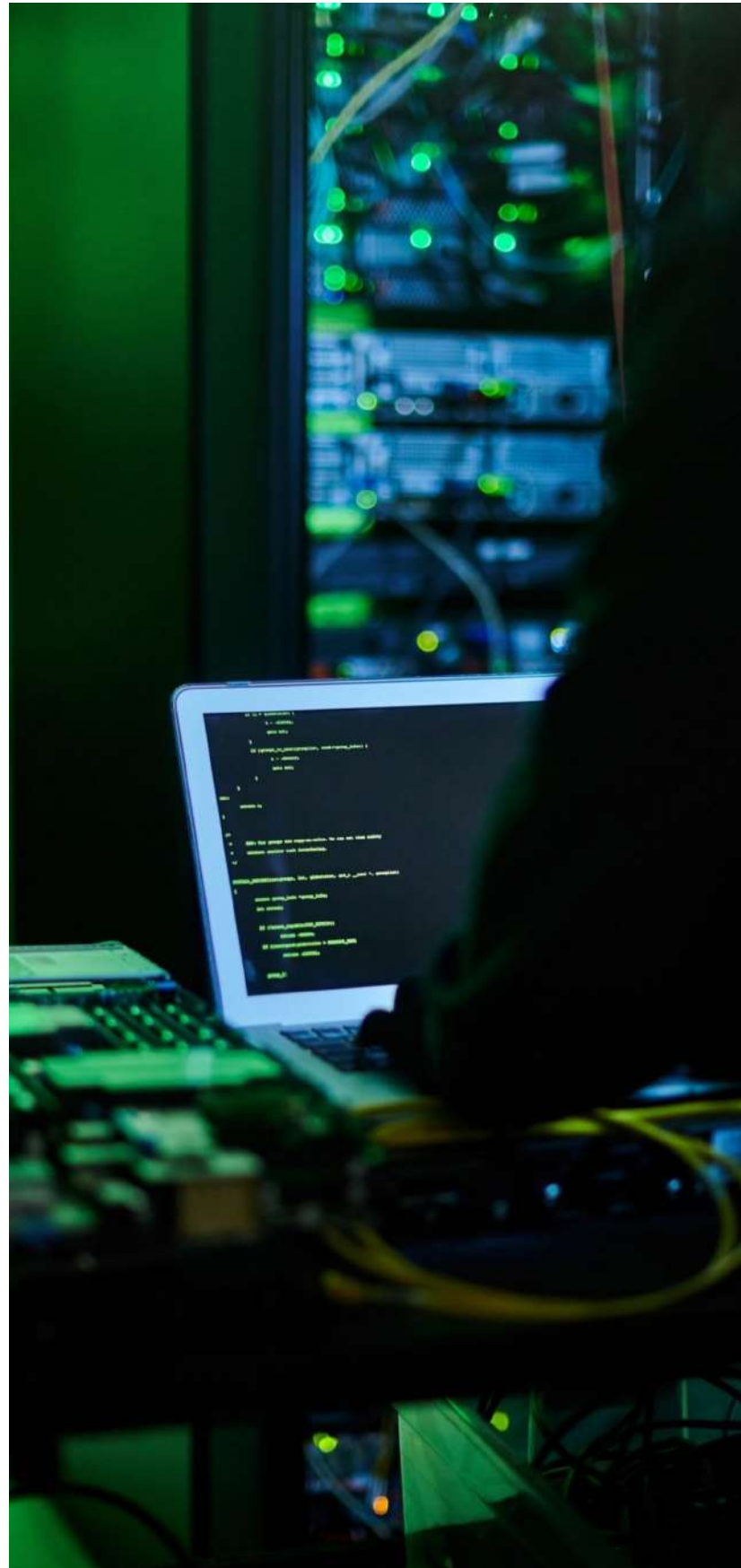
---



**Hiba Sherin T**  
MEA19CS029

## Introduction

Cybersecurity is the technique of preventing harmful assaults on computers, servers, mobile devices, electronic systems, networks, and data. Information technology security and electronic information security are some names for it. The term “cyber security” refers to a group of techniques, tools, and procedures that work together to defend computer systems, networks, and data against hacker attacks and illegal access.



Cybersecurity is important because it helps defend against online attacks on businesses and people. Data breaches, identity theft, and other forms of cybercrime can be avoided with the use of cybersecurity. To protect their consumers' data and information, businesses need to have robust cybersecurity procedures. Millions of people's personal information may be exposed as a result of a single security breach. These violations have a negative financial impact on the businesses as well as a loss of client confidence. Therefore, it is crucial to have cyber security to shield both persons and businesses from spammers and online crooks.

One of the most ground-breaking inventions in recent decades is open-source software. Employing open-source software can aid businesses in maintaining higher levels of technology security. It is simpler for a cybersecurity team to maintain open-source software updated against the most recent flaws than closed-source software since open-source software typically has a smaller development staff.

### **The Potential For Open Source To Improve Cybersecurity**

open-source weapons of defense Every business using an open-source tool would gain from it becoming more widely used because, when one business resolves a bug or contributes code to fortify their systems, they fortify the defense of every other business using the same open-source software.

Larger corporations as well as smaller businesses who would not otherwise be able to build a strong defence benefit from

unifying cyber-protection. These larger businesses frequently make the mistake of investing in cybersecurity products without fully understanding their capabilities. They often believe that their cybersecurity is more secure the more money they have allocated to it. In fact, many of these measures are redundant or superfluous, and even the most effective cybersecurity defences have vulnerabilities. Closing these gaps enables collaboration among cybersecurity tools to produce a united, more effective defence against cyberattacks. An exploit will no longer be usable against any other team if one team resolves it.

Email security and defence are other areas where open source can advance. Affordable and integrated software can be quite helpful in preventing cyberattacks and safeguarding business email. These products can be developed to attain higher standards of quality, stability, and security over a longer period of time than projects that do not use the open-source development paradigm because of the accessibility and transparency of open-source code.

### **Open Source Cyber Security Tools**

#### **1. Nmap**

An open source network scanner called Nmap quickly examines huge computer networks utilised for both service and OS detection and hosting discovery, finds host information on a network by using raw IP packets.

A reliable platform for creating and disseminating unique scripts that solve frequent issues is the Nmap Scripting Engine (NSE). You can select from a wide variety of

easily accessible scripts to carry out rapid network inspections.

Pros:

- Network mapping can be done easily without complicated commands.
- Administrators can easily browse through subdomains and DNS requests.
- Highly adjustable, allowing users to quickly alter the scans.
- Because of its light weight, the start-up procedure is accelerated.

Cons:

- It takes a lot of practice to become proficient in all of Nmap's functions.
- If the network is not limited, scanning may take longer.
- Certain scan types can be aggressive and mistakenly activate IDS/IPS systems.

## 2. Metasploit

Metasploit is a powerful open-source framework for developing, testing, and using exploits. It was originally created as a tool for penetration testing and ethical hacking, but has since become a popular platform for cybercriminals as well.

The Metasploit framework includes a vast library of exploits and payloads, which can be used to attack vulnerabilities in computer systems and applications. The framework can be used to perform various security tasks, such as reconnaissance, vulnerability scanning, and exploitation

Metasploit can be used on a variety of platforms, including Windows, Linux, and

macOS. The framework is constantly updated with new exploits and features, making it a valuable resource for security professionals and researchers.

It's important to note that while Metasploit can be used for legitimate security purposes, it can also be used maliciously. It is illegal to use Metasploit to attack systems or networks without proper authorization, and those who use it for malicious purposes may face criminal charges.

Pros:

- Runs on Windows, macOS, and Linux platforms and is fully cross-platform.
- This open source security tool has great support from the community.
- The codebase is open source and can be used to integrate with other programmes.
- Large-scale security teams can benefit from the pro version's advanced automation features.

Cons:

- The feature-rich free edition is complicated to use and has few options.
- The Windows and Linux versions operate noticeably differently.
- Some vulnerabilities cannot function successfully without user input.

## 3. OSSEC

OSSEC (Open Source Security) is an open-source intrusion detection system (IDS) that helps organizations to detect and respond to security threats in real-time. It is designed



to monitor various log files, system activities, and network traffic for signs of malicious or unauthorized activity. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response. The software can be installed on various platforms, including Windows, Linux, and macOS, and it can monitor both local and remote systems.

OSSEC provides a centralized management console for security events, which makes it easier for administrators to monitor and respond to security incidents. The software also includes a flexible alerting mechanism, which allows administrators to configure custom alerts based on specific security events.

It is widely used by organizations of all sizes and is considered to be a reliable and effective solution for intrusion detection and security event management. It's important to note, however, that like any security tool, OSSEC should be used as part of a comprehensive security strategy and in conjunction with other security tools and best practices

Pros:

- provides proactive actions and real-time alerts for problems.
- It accepts logs in formats from FTP servers, databases (PostgreSQL, MySQL), and web servers, among others.
- CIS and PCI-DSS compliance among other security auditing requirements.
- effectively gathers system data and serves as a system inventory.

Cons:

- Threat visualization may be more difficult in the absence of a monitoring dashboard.
- There can be discrepancies in the rules after upgrading the OSSEC version.
- Miscommunication when using pre-shared keys can be problematic.

#### 4. Kali Linux

Kali Linux is a Debian-based open-source operating system that is widely used by ethical hackers, penetration testers, and security professionals. It is a distribution specifically designed for digital forensics, penetration testing, and security auditing.

Kali Linux comes pre-installed with a vast collection of security tools and utilities, including network analysis tools, web application analysis tools, password cracking tools, and exploitation tools. The distribution also includes a customized graphical user interface, making it easy for users to access the tools they need.

One of the key features of Kali Linux is its rolling release model, which means that the operating system is constantly updated with the latest security tools and features. This makes it an essential tool for security professionals and researchers who need to stay current with the latest security trends and threats.

Kali Linux can be run as a live system, which means that users can test the operating system without installing it on their hard drive. This makes it possible to run the operating system from a USB drive, allowing users to carry it with them and use it on different

systems.

It's important to note that while Kali Linux can be used for legitimate security purposes, it can also be used maliciously. It is illegal to use Kali Linux to attack systems or networks without proper authorization, and those who use it for malicious purposes may face criminal charges.

Pros:

- security professionals work in a specialized setting.
- Included are over 600 penetrating tools.
- Assistance for wireless devices.
- The Debian testing branch is where the

majority of apps are derived from.

- The cloud, containers, Android, ARM, and WSI are just a few of the places you can use it to execute.

Cons:










- steep learning curve; could be challenging for beginners.
- It might often feel sluggish to use some security tools on Kali.
- There is need for improvement in driver support for more devices.

## 5. OpenVAS

OpenVAS (Open Vulnerability Assessment System) is a free and open-source vulnerability

## 10 Best Free and Open-Source SIEM Tools

### What You Need to Know

OSSIM		Offers both server-agent and serverless modes, with log analysis for mail servers, databases, and more.
Sagan		Real-time log analysis and correlation tool that's compatible with graphic consoles like Snorby and EveBox.
Splunk Free		Free version of Splunk tool that lets you index up to 500 MB daily for real-time data indexing and alerts.
Snort		Analyzes network traffic in real time, but features make it best-suited for experienced IT professionals.
Elasticsearch		Combine log search types and easily scan through large volumes of logs with this basic tool.
MozDef		A microservices-based tool that can integrate with third-party platforms for straightforward security insights.
ELK Stack		Combines Elasticsearch with tools like Kibana, Beats, and Logstash, for a fuller SIEM solution.
Wazuh		An on-premises tool that offers threat detection, incident response, and compliance support.
Apache Metron		Combines security operations center functions into one centralized, dynamic tool for catching threats.

scanning and management tool. It can be used to perform vulnerability assessments on various systems, including networks, servers, and applications, to identify and prioritize security risks.

OpenVAS uses a database of known vulnerabilities and exploits, as well as network and system scanning tools, to detect potential security threats. It can also perform tasks such as patch management and reporting. The tool is highly customizable and can be integrated into larger security infrastructures. OpenVAS is a popular choice for network administrators, security professionals, and organizations looking for a cost-effective and flexible solution for managing and reducing the risk of security vulnerabilities.

#### Pros:

- use a list of NVT (Network Vulnerability Test) feeds that is continuously updated to do vulnerability tests.
- Excellent for Small Businesses.
- Testing and CVE coverage for bugs.
- a sizable and devoted community, so getting help is simple.
- OpenVAS's open source license allows for third-party customisation.

#### Cons:

- requires much work to get this vulnerability scanner up and running.
- does not provide any cloud scanner for AWS, Azure, or GCP.

## Conclusion

Open source software tools play a critical role in cybersecurity, but they also present some challenges that must be addressed:

- Quality control: Open source tools are developed by a community of volunteers and are not subject to the same quality control standards as commercial software. This can lead to bugs and vulnerabilities that can be exploited by attackers.
- Lack of support: Open source tools may not have official support from the developers, leaving users to rely on community support. This can be a challenge for organizations that require a high level of technical support.
- Complexity: Open source tools can be complex and difficult to use, requiring a certain level of technical expertise to set up and maintain.
- Integration: Open source tools may not integrate seamlessly with existing systems and processes, requiring additional effort to integrate them into an organization's cybersecurity strategy.

Despite these challenges, the importance of open source tools in cybersecurity cannot be overstated. They provide a cost-effective and flexible solution for identifying and mitigating security risks, and they allow organizations to benefit from the collective knowledge and expertise of a large community of developers and users.

In conclusion, while open source tools in cybersecurity present some challenges, they also provide significant benefits and are an essential component of a comprehensive cybersecurity strategy. Organizations must carefully consider the trade-offs and ensure that they have the necessary resources and expertise to effectively manage and utilize open source tools.



# Dark Web

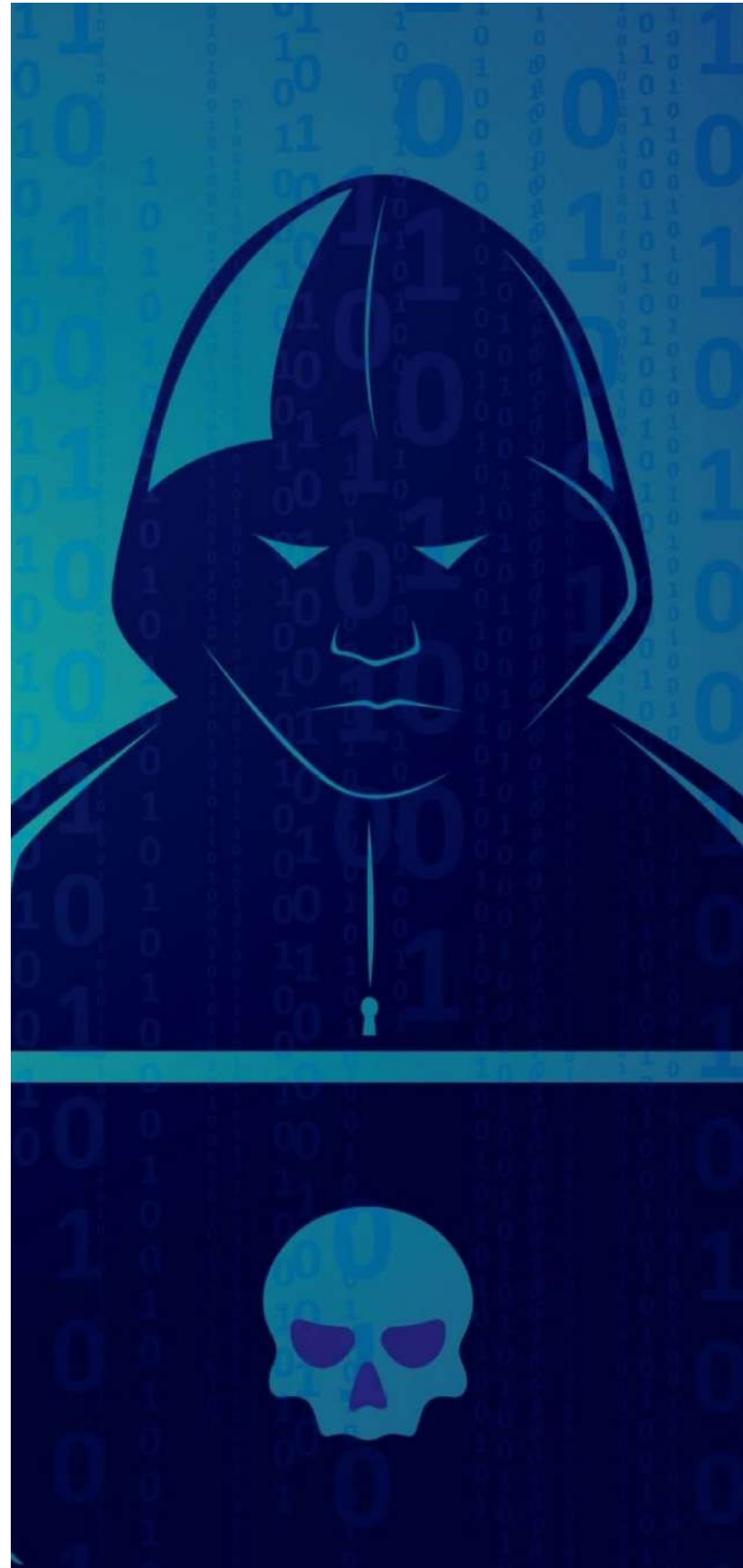
---



**Safvan Melethil**  
MEA20CS079

## Introduction

The dark web is part of the Internet that isn't indexed by regular search engines, like Google, Bing and Yahoo. You won't be able to access the dark web through standard web browsers like Google Chrome or Firefox; instead, you need a special browser called Tor. Any type of information can be found on the dark web. It is only considered "dark" due to the limited accessibility and anonymity that comes with using Tor.



To best understand what the dark web is, it is important to know that the Internet is made up of three main parts – the open (or surface) web, deep web and the dark web.

## Types of Web

The surface web – this is what makes up around 10% of the Internet and includes everything and anything that can be found via search engines like Google. Things like Facebook, Amazon and Wikipedia are all part of the surface web.

**The deep web** – despite the menacing name, the deep web is merely part of the Internet that isn't easily accessed without passwords etc. This can include things like your email account, pages you use to do online banking, company servers and even blog posts that are saved as drafts in WordPress. The deep web makes up the majority of the web.

**The dark web** – this is the part of the web that is only accessible through an onion router like Tor. Sites on the dark web are easily recognised by the “.onion” domain name, and they usually contain content that users don't want to be found by Google. This can include anything from drugs and guns for sale to surveillance conscious blogs or anonymous government critics.

## Dark web is used for what?

### 1. Anonymisation

People may have many reasons for protecting their online identity. In some cases, this is because they would be in danger if their identity became known – for example in countries where the government forbids a free press or where there is political censorship.

Others may use it to reduce their risk of falling victim to crime, such as people who have been cyber-stalked or who are concerned about the security of online banking. Tor is mainly used for people to browse the open web anonymously, a very small percentage of its traffic relates to Hidden Services (below).

### 2. Accessing 'Hidden Services'

A Hidden Service (also known as an 'onion service') is one where not only the user, but also the website itself, have their anonymity protected by Tor. This means that the IP address of the site cannot be identified, meaning that information about its host, location or content is hidden. Hidden Services are sometimes called “onion addresses” because the website name often ends on .onion.

Tor itself is not a Hidden Service, but the sites it hosts are. Hidden Services can be used legitimately, for example for whistleblowing or to allow members of the public to share sensitive information such as knowledge about crimes without the risk of reprisals. However it is generally believed that the majority of Hidden Services contain illicit material. They often require registration (username, password etc) and some have 'VIP' sections, accessible only by an invite from the administrators or through an application made by the member and approved by the administrators.

### 3. Illegal Activity

The Dark Web may be used by people wishing to carry out illegal activities online, such as selling weapons or drugs. These kinds of operations, and the websites offering them, are often referred to as Hidden Services

(above).

### What are the risks?

In many ways, the risks of the ‘Dark Web’ are the same as those that may be encountered in the ‘Open Web’. Young people in both environments may access pornography, indecent images of children, or sites selling drugs and weapons.

Young people are also at risk of exploitation and abuse by sex offenders who use all parts of the internet to target victims. However, there is evidence to show that offenders are more likely to interact with victims on the ‘Open Web’ than on the ‘Dark Web’. The Dark Web is more commonly used by sex offenders to openly discuss ‘tactics’ to exploit young people and share material generated as a result of their offending. It is also harder for law enforcement to investigate online abuse that takes place in the anonymous parts of the internet.

### Dark Web vs. Deep Web: What’s the Difference?

Most of the digital content in the world is not accessible via web search engines.

This colossal amount of information exists on the Deep Web (or “hidden web”), where almost all online activities take place.

You actually use the Deep Web as part of your daily routine. Every time you log into your email account, check out your online banking details, or use social media, you’re on the Deep Web.

The Deep Web hosts information that usually requires a username and a password to access, mainly for security and privacy-related reasons.

Many of the activities on the Deep Web involve

personally identifiable information, such as medical and legal documents, financial records, academic research, intellectual property, confidential commercial data, and more.

While you may not be using the term Deep Web daily — or ever — it’s part of your life more than you realize.

Still, this is not the same as the Dark Web, a term you’ve likely seen around. The Dark Web is yet another fraction of the internet that’s not equivalent to the Deep Web. Let’s look at the reasons behind its negative reputation.

### Why is the Dark Web So Dangerous?

Cybercriminals and other malicious actors rely heavily on the capabilities of the Dark Web in various unlawful ways. The hotspots for illegal activity on the Dark Web are marketplaces and forums where bad actors transact illegal products and services, which fuel the underground economy.

Some of the illicit products lawbreakers and scammers sell and buy on these black markets include stolen and counterfeit data which comes in many varieties:

- Personal data. (Also called PII, personally identifiable information) which includes full names, home addresses, phone numbers, birth dates, Social Security numbers, hacked email address and many more details that can pinpoint you as an individual.
- Financial data. Stolen credit card details, online banking usernames and passwords, credentials for cryptocurrency accounts, banking and insurance records, and much more.
- Online account login data. Typically



composed of username-password combinations, which provide access to accounts ranging from social media to ride sharing and video streaming services to paid professional services — including genetic testing and even antivirus products.

- Medical data. (Also called PHI, personal health information) which covers your medical history, prescriptions, biometric data (including your fingerprints and images of your face), test results, billing information from medical facilities, and other sensitive details. This can lead to medical identity theft or even fingerprint identity theft.
- Confidential corporate data. Includes classified information such as intellectual property, patents, competitive intelligence, and other operational details.
- Forged data. Most notably fake passports, stolen drivers license and IDs, bank drafts and more.

Besides personal information yielded from data breaches and various other types of cyber attack and online scam, these black markets also offer illegal drugs, access to emerging cyber threats and viruses, and even hitman for hire.

The most notorious of all Dark Web marketplaces was Silk Road which, at its peak, catered to over 100,000 buyers. Founded by Ross Ulbricht in 2011, the website became the most popular black market, especially for narcotics traffickers. The FBI shut down Silk Road in 2013, but version 2.0 came briefly back online before law enforcement took it down for good.

Ross Ulbricht received two sentences of life

in prison, along with three other convictions, and the U.S. government seized over \$1 billion worth of bitcoin throughout the entire takedown operation and the decade following it.

In addition to the possibility of making big money on these Dark Web marketplaces, people seek the Dark Web for other reasons as well. This part of the internet also hosts vast amounts of child pornography, with some websites reaching tens or hundreds of thousands of users.

As a hub for criminal activity, the Dark Web offers more than just “products” to anyone willing to buy and consume. It also offers services that enable cyber-criminals to launch attacks with little technical knowledge or experience.

## Conclusion

In sum, the Dark Web poses a cyber-security risk to anyone on the Internet. Though accessing the Dark Web to patrol for your personal information is not advisable, being aware of its potential impact in facilitating cybercrime is important in developing a sound cyber-security protocol. Limiting the sharing of personal information, staying apprised of recent cyber threats including ransomware, and following steps to mitigate risk in the wake of high-profile data breaches are all great steps in a proactive approach. Additionally, acknowledging the slippery slope of questionable “gateway” sites to the Dark Web can help keep you and your family safe from what the Dark Web encompasses.

## Pros of Dark Web

**Knowledge** - The Deep Web is a treasure-trove of information and knowledge. It has

some of the largest virtual libraries, more than you can possibly fathom. The knowledge available on the Deep Web is often accessed by teachers, students, and researchers as it is not so readily available on standard search engines. Scientific data that has been kept hidden from the public eye can be easily found in the Deep Web by spending some time researching it.

**Anonymity** - While some consider anonymity to be a double-edged sword, it should be appreciated positively as it results in freedom. Browsers that are used to access the Dark Web, such as Tor, are secure as they guarantee that your IP address remains untraceable. To make it more secure, always use Tor with an underlying VPN.

**Freedom of Speech** - As discussed in the preceding point, freedom of speech is one of the most important freedoms that are a direct consequence of anonymity. Some countries practice the right to freely express their

thoughts and opinions very strongly without fearing any form of persecution. This right still remains a utopia for most of the world. Dark Web allows users to freely communicate without fearing law enforcement or government agencies as the communication is encrypted and IP addresses are masked to protect their identity.

**Political Activism** - The 21st century has seen a rise in right-wing oppressive governments around the world that are trying to curtail opposition and free speech. For such regimes, information control is a powerful tool and they track the movements and activities of their citizens on the internet. In many countries, governments are at the liberty to block certain websites as per their choosing, mostly done for social media websites. To counter this, you can use browsers such as Tor that allow users to access even the blocked websites and denounce the oppressive governments.



# CLOUD SECURITY

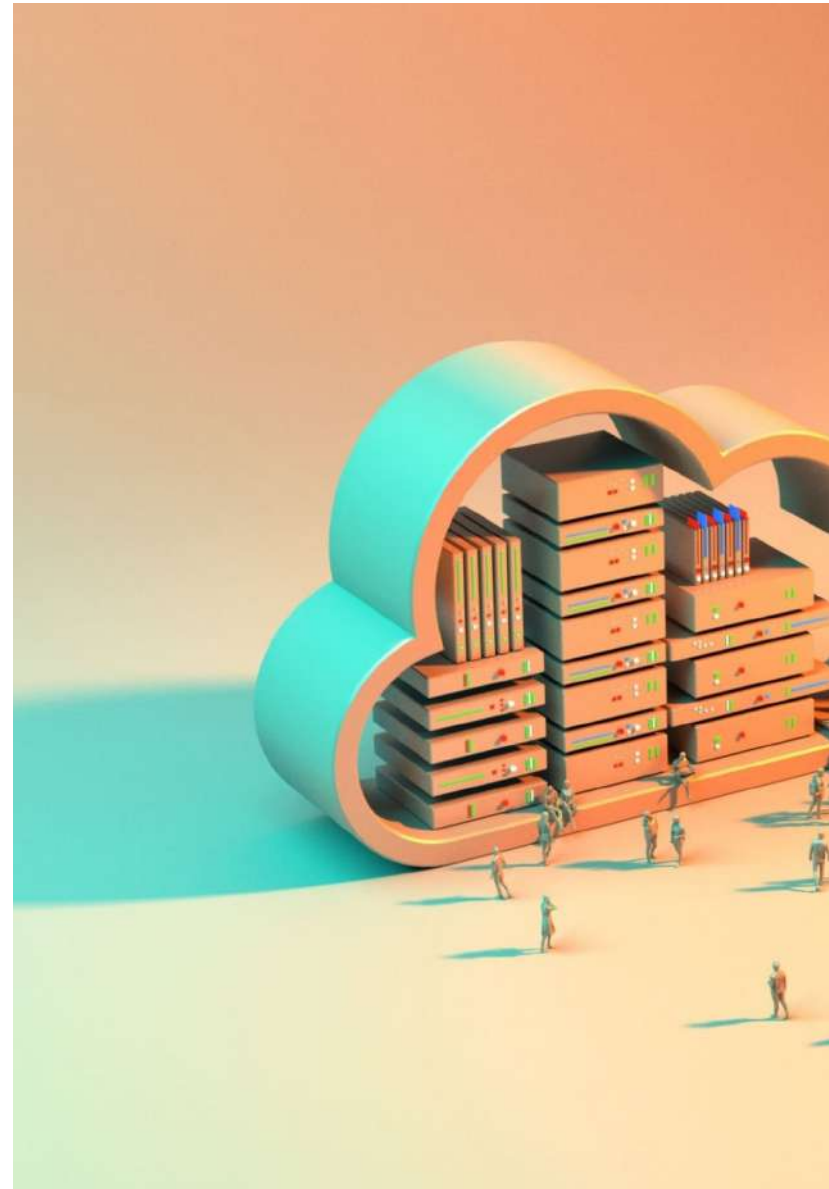
---



**Lena Fathima**  
MEA21CS035

## Introduction

Cloud security is a type of cyber security that focuses on keeping cloud computing systems safe. This includes ensuring the privacy and security of data across internet infrastructure, apps, and platforms. Cloud providers and clients, whether individuals, small to medium businesses, or enterprises, all contribute to the security of these systems. Cloud providers use always-on internet connections to host services on their servers. Because their firm



relies on consumer confidence, they use cloud security to keep client data private and secure. However, cloud security is partially in the hands of the customer. A robust cloud security solution requires an understanding of both aspects.

## Application

Cloud security is made up of the following categories at its core: Data security, Identity and access management (IAM), Governance



(policies on threat prevention, detection, and mitigation), Data retention (DR) and business continuity (BC) planning Legal compliance. Although cloud security may appear to be similar to traditional IT security, this architecture necessitates a different strategy. Let's first define cloud security before going any further.

Cloud security is a sort of cyber security that focuses on ensuring the safety of cloud

computing systems. Ensure data privacy and security across internet infrastructure, apps, and platforms. Individuals, small to medium organizations, and corporations, as well as cloud providers and clients, all contribute to the system's security. Because data breaches occur when services are mistakenly exposed to the public internet, misconfiguration of application setup is the single biggest threat to cloud security.

Here are five top practises for creating effective security measures in cloud applications:

### **Identity access management (IAM)**

IAM ensures that every user is authenticated and can only access data and application capabilities that they are permitted to see. A holistic approach to IAM helps safeguard cloud apps while also improving an organization's overall security posture.

### **Encryption**

Encryption in the correct places improves application performance while safeguarding sensitive data. Encryption in the correct places improves application performance while safeguarding sensitive data. Encryption in transit, encryption at rest, and encryption in use are the three types of data encryption to consider.

### **Threat monitoring**

This allows development teams to identify and address cloud application security problems before they affect end users.

### **Data privacy & compliance**

Data privacy and compliance, in addition



to application security, are critical for protecting end-users of cloud native apps. Furthermore, data encryption, access limits, and other cloud security controls can assist protect app users' privacy.

### **Automated security testing**

Integrating automated security testing into the development process is an important aspect of DevSecOps. Development teams may verify that every new software build is secure before delivering to the cloud by automatically screening for vulnerabilities during the continuous integration and continuous delivery (CI/CD) process. This covers not only the applications code and open source libraries, but also the container images and infrastructure configurations they need for cloud deployments.

### **Why is cloud security so crucial?**

Business and personal data were stored locally in the 1990s, as was security. If you worked for a firm, your data would be stored on enterprise servers and on the internal storage of your PC at home. The introduction of cloud technology has made everyone rethink their cyber security. Your data and apps could be bouncing around between local and remote computers, always connected to the internet. That data might be stored anywhere if you use Google Docs on your smartphone or Salesforce software to manage your customers.

Convenience takes precedence over security. Cloud computing is rapidly becoming a popular solution for both business and personal use. New technology is being introduced at a faster rate than industry security regulations can catch up, putting additional responsibility on users and

providers to consider accessibility hazards.

Storage with multiple tenants and centralization. Every component, from fundamental infrastructure to minor data like emails and documents, may now be located and accessed remotely via web-based connections that are available 24 hours a day, seven days a week. All of this data gathering on a few major service provider systems can be quite harmful. Large multi-organizational data centers can now be targeted by threat actors, resulting in massive data breaches.

### **24x7 Visibility**

The top cloud security solutions, such as AppTrana, provide for round-the-clock monitoring of applications and cloud-based assets. This enables enterprises to maintain a constant view of their risk posture and its impact on the business.

### **Increased Availability**

The majority of cloud computing security solutions feature built-in redundancies to ensure that the application /resources are always available. The CDNs used have distributed worldwide networks of edge servers that provide content efficiently, improve application speed, and reduce server access. They handle traffic surges better than on-premises /hardware solutions.

### **Effective protection against DDoS Attacks**

DDoS attacks are rising in frequency, volume, sophistication, and intensity, and cloud security solutions provide the most effective defense against them. DDoS attacks are constantly monitored,

identified, analyzed, and mitigated with the help of cloud computing security. Such solutions can prevent volumetric, low and slow attacks. Because of their built-in redundancies, customizability, flexibility, scalability, and intelligence.

### **Data Security**

Data security is designed into the top cloud computing security solutions. To prevent unauthorized entities from obtaining confidential information, they use security methods and policies such as rigorous access controls and data encryption.

### **Pay as you Go Model**

Rather than making a large upfront commitment, the cloud security model ensures that you only pay for what you need and consume.

### **Advanced Threat Detection**

Cloud computing security can more quickly detect vulnerabilities by leveraging end-point scanning and global threat intelligence. This aids in measuring the threat landscape's impact on the organization's mission-critical assets.

### **Regulatory Compliance**

Top-tier cloud app security providers aid in meeting regulatory requirements and industry-specific compliance requirements. This is accomplished through the company's improved infrastructure and managed security services.

## **Conclusion**

Despite the fact that many firms still assume on-premise and hardware-based security is

more safe, this is not the case. Because cloud computing is still new, the security threats are mainly unknown. If your company uses cloud apps or is considering making the move to the cloud, you should be aware of the security requirements. You'll also need access to the visibility and control you have with on-premise software in terms of access and use. The advantages of cloud security are numerous, demonstrating how cloud security outperforms on-premise security. To ensure the enhanced security of your cloud-hosted assets, choose the correct cloud security supplier. To learn how it works, start with the AppTrana Free Forever Website Security Scan.

## **Top Rated Cloud Computing Security Products**

These products were given the top rated distinction because of their high customer satisfaction ratings. The list is entirely based on user reviews, there is no paid advertising, and analyst opinions have no bearing on the results.

- Check Point CloudGuard.
- CloudPassage Halo.
- Threat Stack Cloud Security Platform.
- Symantec Cloud Workload Protection.
- Datadog.
- HyTrust.
- PaloAlto Prisma.
- Fortinet.

Cloud adoption is quickly increasing, assisting firms with scalability, expansion and agile development. Cloud technology has become a need in the post-COVID era and cloud security is a real concern.

# VULNERABILITY OF IOT



**Mohammed Binshad P**  
LMEA19CS097

## Introduction

The necessary internal security needed to defend against security attacks is missing from the average IoT device.

Because of widespread flaws and exposures, hackers can get inside the system and utilize it as a base for complex cyberattacks.

### Significant IoT threats to devices include:

1. IoT devices have limited processing and hardware capabilities, leaving little room for the robust data protection and security required to defend against cyberattacks.
2. Different transmission technology: IoT devices employ a variety of transmission technology, making it difficult to adopt adequate security procedures and protocols.
3. Vulnerable components: IoT devices basic components are frequently exposed, leaving millions of smart gadgets vulnerable to assault.





4. Users' security awareness is one of the most significant security threats.
5. IoT devices might be vulnerable to attacks due to a lack of security awareness and inability to follow best practices.

### How Do IoT Devices Vulnerabilities Affect Users?

Cyber criminals search for vulnerabilities in IoT devices to launch attacks on organizations and end-users. Examples of how IoT device

vulnerabilities can affect users include:

1. **Lateral network movement:** The initial breach of a vulnerable device might be used by cyber criminals to gain access to business networks. An attacker attempts to exploit a machine's vulnerability before gaining elevated privileges. They then employ lateral movement to gain access to sensitive information and propagate malware across a network
2. **IoT botnets:** Botnets, which are huge networks of devices such as routers, are used by cyber criminals to perform large-scale assaults such as distributed denial-of-service (DDoS) attacks. Botnets are a collection of infected devices controlled by a command-and-control server. In 2016, the Mirai botnet, for example, shut down a number of important services and websites, including gaming services. Mirai used a botnet code that was put into the wild for other hackers to exploit to target unsecured devices.
3. **Evolving botnets:** Botnets may evolve and become an even greater hazard to people as the Internet of Things grows. This could happen as a result of peer-to-peer (P2P) file-sharing technologies, which allow an attacker to link devices without the need for a central server, making prevention nearly difficult.
4. **Household devices:** Connected appliances, digital assistants, wearables, health monitors, and other IoT devices are gradually pervading the house. Other devices connected to home networks, such as laptops and computers, may be vulnerable to IoT service vulnerabilities. Hackers may be able to obtain access to corporate networks if these devices are



utilized to work from home or as part of a bring-your-own-device (BYOD) policy.

**5. Existing device issues:** To get access to internal networks, attackers can target IoT devices with known vulnerabilities. They can then carry out operations such as DNS rebinding attacks to steal data from networks and devices connected to household or corporate networks.

### **Vulnerabilities of IoT applications:**

IoT apps are vulnerable to a number of flaws that put them at danger of being hacked, including:

**Weak or hardcoded passwords:** Many passwords are easy to guess, publicly accessible, or unchangeable. Some IT professionals don't bother updating the device or software's default password.

**Lack of an update process or mechanism:** Because many IoT apps and devices are invisible on the network, IT administrators accidentally block them from updates.

Also, due to their age or function, IoT devices may not have an update mechanism built in, preventing administrators from updating the software on a regular basis.

**Unsecured network services and ecosystem interfaces:** Each IoT app connection has the potential to be hacked, either due to a flaw in the components themselves or because they aren't protected against assault.

Any gateway, router, modem, external web app, API, or cloud service connected to an IoT app falls under this category.

### **Outdated or unsecured IoT app components:**

Many IoT apps are built using third-party frameworks and libraries.

They could be a security issue if they're outdated or contain known flaws and aren't evaluated before being put in a network.

### **How to protect IoT applications**

IoT app security requires a multi-step procedure. It demands planning, doing, and constant observation. Start by considering these ideas:

#### **Learn the most likely threats**

Threat modeling can be used to find, rank, and evaluate potential IoT app vulnerabilities. To guarantee that IT managers incorporate IoT apps in their overall security strategy, a model can suggest security measures. The model should develop and vary over time in order to accurately reflect the state of the IoT app..

#### **Understand the risks**

Not all threats are the same when it comes to IoT applications and a business. Prioritize risks based on their seriousness and take the necessary action. Many tech teams undervalue the significance of aligning risk with business outcomes and scenarios. Although an IoT app failure or compromise might seem insignificant to IT, the company could suffer serious financial repercussions.

#### **Update apps regularly**

IT administrators need to deliver updates to IoT apps as soon as they are ready in order to maintain the security of the network. Use only authorized and verified updates, and while updating apps over the air, encrypt all

update data streams using a VPN. Secure public key infrastructures can also be used to authenticate devices and systems (PKIs).

#### **Secure the network**

Firewalls, encryption, and secure connection protocols shield IoT programmes from unauthorized access. Review the various devices, standards, and communication protocols used on the network on a frequent basis to ensure optimal security. IoT apps should be considered in any assessment of application security.

#### **Conclusion**

To take preventative action, it is necessary to understand the several threats that IoT faces. In this essay, we spoke about IoT security issues and risks. The final goal was to characterize potential dangers, attacks, and vulnerabilities that the Internet of Things might face while also identifying strengths. With a focus on security vulnerabilities linked to IoT devices and services, a summary of the most urgent IoT security issues was presented.



# JOB OPPORTUNITIES IN CYBER SECURITY

---



**Asheeq Akthar C**  
MEA21CS014

## Introduction

Cybersecurity refers to the process of protecting critical systems and confidential information against digital threats. Cybersecurity measures, also known as information technology (IT) security, are designed to prevent threats to networked systems and applications, whether they come from within or outside of a company. Cybercrime is on the rise, highlighting faults in the devices and services we've grown to



rely on. This concern leads us to contemplate the significance of cybersecurity, its purpose, and the lessons we can gain from it.

Government, military, corporate, financial, and medical entities all collect, process, and store massive amounts of data on computers and other devices, making cyber security critical. A considerable amount of such data may be sensitive information, such as intellectual property, financial data, personal





information, or other sorts of data that could be harmed by illegal access or exposure. In the course of doing business, companies send sensitive data via networks and to other devices, and cyber security refers to the discipline committed to safeguarding that data and the systems that process or store it. The cyber security sector nowadays is primarily concerned with defending devices and systems against hackers. While the bits and bytes driving these efforts are difficult

to visualize, the implications are much easier to consider. Many websites would be practically impossible to use if cyber security professionals did not work ceaselessly to prevent denial-of-service attacks. It would be easy to destroy modern-day essentials like electricity grids and water treatment facilities if there were no strong cyber security defenses in place. In essence, the protection of our way of life is heavily reliant on cybersecurity.

### **Jobs In Cyber Security**

Jobs in cybersecurity are exciting. This fast-paced field is ideal for anyone who enjoys a challenge and the thrill of solving problems. According to the Bureau of Labor Statistics (BLS), demand for cybersecurity positions such as information security analysts will increase by up to 31% in the next 10 years.

The demand for experienced cybersecurity specialists is growing as technology becomes more and more integrated into everyone's daily lives. While future cybersecurity employment estimates show more openings, the reality is that there aren't enough competent specialists to go around right now. Because the cybersecurity job market has evolved so quickly in recent years, candidates typically have a wide range of possibilities. Because of the scarcity of skilled professionals, those who pursue a career in cybersecurity may expect numerous job chances, high compensation, and excellent perks. From entry-level positions to executive management and all in between, the cybersecurity profession offers a wide range of opportunities.

A security analyst in a SOC (security operations center) is a position that an entry-



level security professional might find oneself in . They might work as a senior security analyst or on an incident response (IR) team as their career grows. A career as a security software developer is a good fit for those who enjoy programming and software design. A computer forensics career could be an excellent fit for those who want to combine their passions for law enforcement with technology. In order to examine cases, computer forensics experts collaborate with both law enforcement and commercial firms. Many career opportunities for cybersecurity specialists exist across industries, including banking, education, content management, and IT services.

### **Skills Required to Become a Cyber Security Analyst**

Different professions in the cyber security area need different skill sets that people must master in order to succeed in their careers. You'll mostly be required to have advanced technical abilities, such as programming languages. The following are some of the most important programming languages to be aware of :

- Python.
- Android.
- IoT.
- Cryptography.
- Virtualisation Network Services and Security.
- Windows Server

### **Career Prospects in Cyber Security**

In this modern world, cybersecurity is an essential field. With the recent increase in cyber-attacks, ensuring the security of your and your clients data has become a must-

have for all

businesses. There are several cyber security careers available which are listed below :

#### **1. Security Engineer**

Patching, maintaining, and removing items from the system are all tasks that security engineers perform. They work on the system directly and are in charge of its modification.

#### **2. Security Specialist**

Security specialists are those who are in charge of the safety of their companies. They look for any security vulnerabilities in the systems and networks. Because a security professional is necessary to examine cloud systems on a regular basis, the emergence of the cloud trend has boosted this role.

#### **3. Security Consultant**

Security consultants examine systems and make recommendations for enhancements while pointing out weaknesses. These individuals usually work as freelancers to create a security Plan.

#### **4. Incident Responder**

People who recognise and respond to risks are generally considered as incident responders. These individuals assist the company and its workers in remaining prepared and responding quickly when security is compromised.

#### **5. Penetration Tester**

Penetration testers are those who are permitted to hack into a system and try to get access. They act as if they are hackers trying to breach the security system.

#### **6. Forensic Expert**

Hackers and breaches are traced back by forensic experts. They look into cyberattacks and any other unlawful conduct that occurs on the internet. They attempt to recover any

data relevant to the crime that has been corrupted or encrypted.

### **7. Security Auditor**

Security auditors are in charge of discovering a system breach before anybody else. They examine if the firewalls and other security measures in place are functioning properly.

### **8. Security Analyst**

Security analysts examine the systems and fix the flaws. They frequently collaborate with the rest of the IT specialists and developer team.

### **9. Security Architect**

Security architects, as the term indicates, are those who design the security framework. They also do security tests and respond to attacks.

### **10. Security Manager**

The rest of the staff is led by security managers. They make key choices and supervise the work of the entire team.

### **11. Cryptographer**

Cryptographers utilize cryptography techniques to encrypt and decode data, keeping it concealed from unauthorized parties. They are extremely important and in high demand.

### **12. Vulnerability Assessor**

People who run numerous tests on systems are known as vulnerability assessors or vulnerable assessment analysts. Their primary goal is to identify serious security problems while also prioritizing issues that have a major impact on the enterprise.

### **13. Security Administrator**

The most important individuals are security administrators. Their responsibilities involve a variety of titles. They are in charge of establishing suitable data flow security principles as well as implementing firewalls

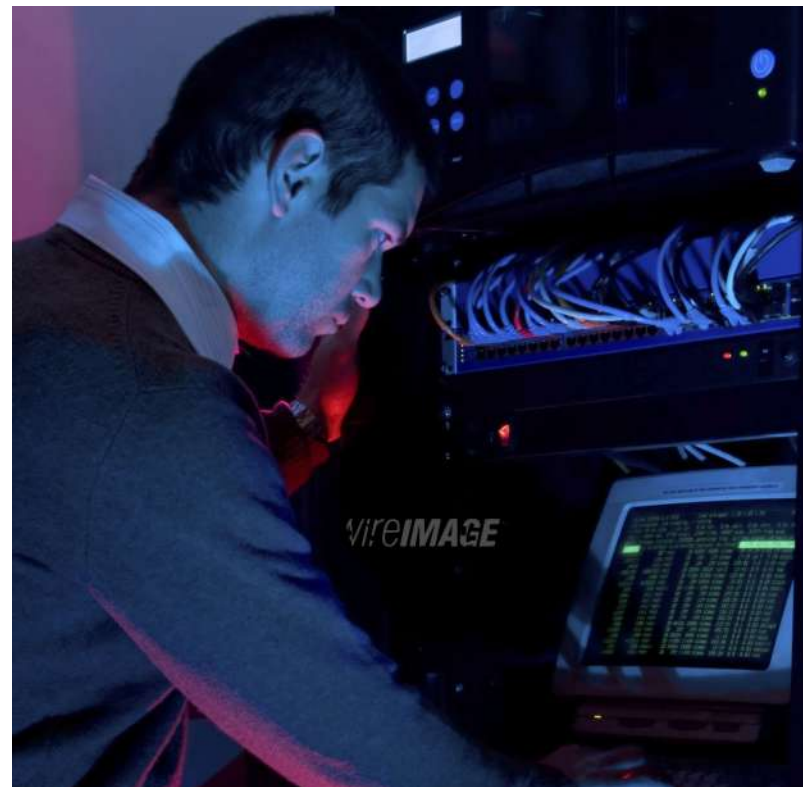
and virus blockers.

## **Conclusion**

The top five industries for cybersecurity specialists, according to the SANS report, are banking, finance, insurance, information technology, government (defense), government (nondefense), and consulting/professional services.

These top industries all deal with sensitive information, which is frequently the target of attackers, which is not surprising.

Since there has already been a significant increase in these positions and skill sets, it is safe to argue that the rise of cybersecurity roles is only getting started. Increasing security training can enhance the skill sets of existing professionals, and expanding security programs in universities can attract and prepare new generations for such roles.



# SECURITY IN BIOIN- FORMATICS

---



**Shahma K P**  
MEA21CS085

## Introduction

Bioinformatics is the study of biological processes and data using computer tools. Bioinformatics is the study of creating and exploiting computer databases and algorithms to speed up and improve biological research. It involves analyzing biological data using computers and statistical approaches. Genomes, proteomes (protein sequences), three-dimensional models of biomolecules, and other biological systems are all examined



using bioinformatics. Even though there are countless potential applications for this type of computational analysis, the majority of current research is concentrated on creating effective ways to store, process, and manipulate enormous amounts of data as well as on creating and analyzing models of important molecular, physiological, and ecological systems. Both commercially and academically, bioinformatics has the potential to be employed in the fields of medicine,



agriculture, and biology since patterns found in samples and modeling can be used to develop and improve treatments, goods, and services.

### **Security Threads**

Researchers have made amazing strides in understanding and treating disease because of the expanded use of large-scale genomic databases, but it has also raised concerns about prejudice and loss of privacy.

Bioinformatics and computational genetics have prompted many ethical issues. Genetic data kept in a bioinformatics computer system can be used to identify a person. This privacy concern is due to the possibility that private medical information or other information that might be used to harm a person could be made public in the case of a data breach. As a result, it possesses a huge collection of sensitive data that is vulnerable to invasions of privacy. These delicate characteristics have led to the development of ethical guidelines for the distribution of genetic data.

Health information, both in its paper and electronic forms, is used for a multitude of purposes by an array of individuals and organizations internal and external to the healthcare industry.

- The primary users of such data include doctors, nurses, physicians, clinics and hospitals that provide care for patients.
- Secondary users are often those who utilize and organize this health information for an assortment of business, societal and government purposes—outside of providing care.

Organizations that pay for healthcare benefits, such traditional health insurance firms, managed healthcare providers, and government programmes like Medicaid and Medicare, are among these users. As part of their management responsibilities, these secondary users and payer organizations also analyze the quality of healthcare delivered by such organizations in relation to its expenses. Researchers in the fields of social science and medicine, social welfare and rehabilitation



initiatives, pharmaceutical firms, public healthcare providers, marketing companies, the judicial system, and even the media are examples of other secondary users.

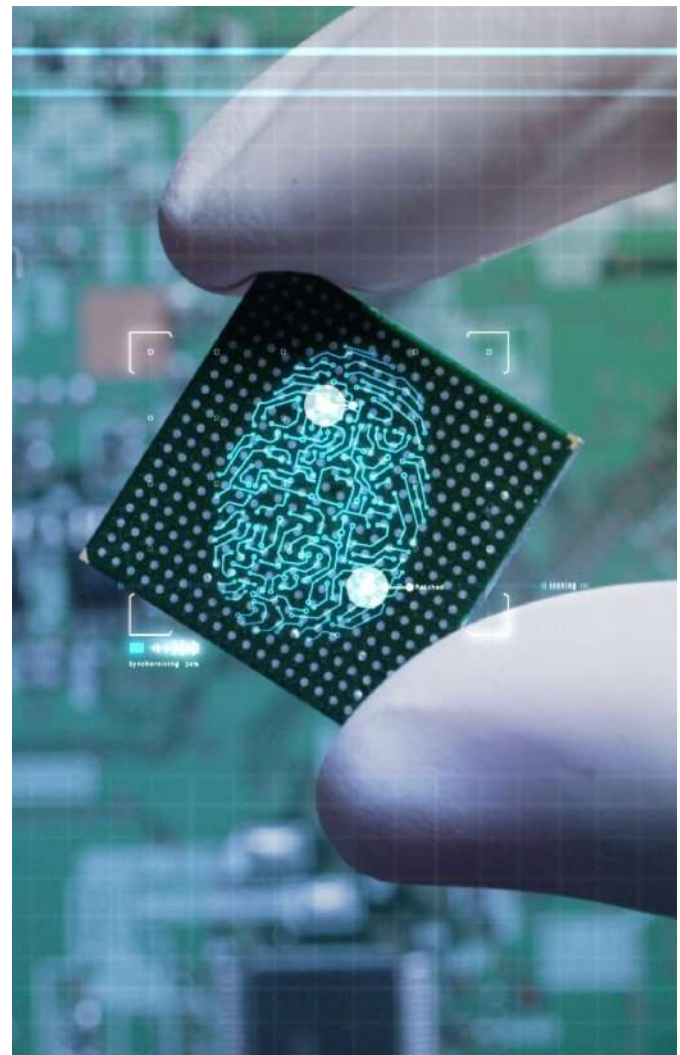
### **Secure Methods for Storing and Transferring Data**

In addition to attempting to preserve the integrity of the data itself, businesses and researchers need to safeguard their commercial or academic interests in a field that is becoming more and more cutthroat. Therefore, it has become crucial to create more secure means of data storage and transit. Various approaches have been developed, depending on the data's privacy needs, the data consumer's privacy requirements, and the mechanism of data exchange. Another proposal is to create a "trusted third party" that may be utilized to store data safely yet conveniently or to transmit encrypted data while keeping input and query anonymity. It's noteworthy to notice that despite the intended level of data protection being increased by these suggested solutions, the industry's intrinsic desire to keep data accessible and shareable is still clear. Since it is recognised that larger and more complete data sets allow for higher-quality analysis, the data are still available, but in a secure format.

### **Conclusion**

Bioinformatics, which is routinely used by the healthcare system to manage enormous volumes of patient data, is increasingly being used in international collaborations aimed at understanding disease states and normal physiology for commercial aims. Both computer scientists and biologists may have greater career options as a result

of the anticipated growth of the field of bioinformatics. Excellent working examples of databases that have been created and are currently in use are the GenBank and PubMed databases. It provides benefits for health and the economy, but it also has drawbacks for the environment and consumer health. In conclusion, the study of genetic traits, biotechnology, and medicine have all greatly benefited from bioinformatics and computational genomics. We currently possess the improvements required to find new treatments and medications. However, these advances and advancements in human life frequently come at the expense of disclosing private biodata.



# Mobile Hacking



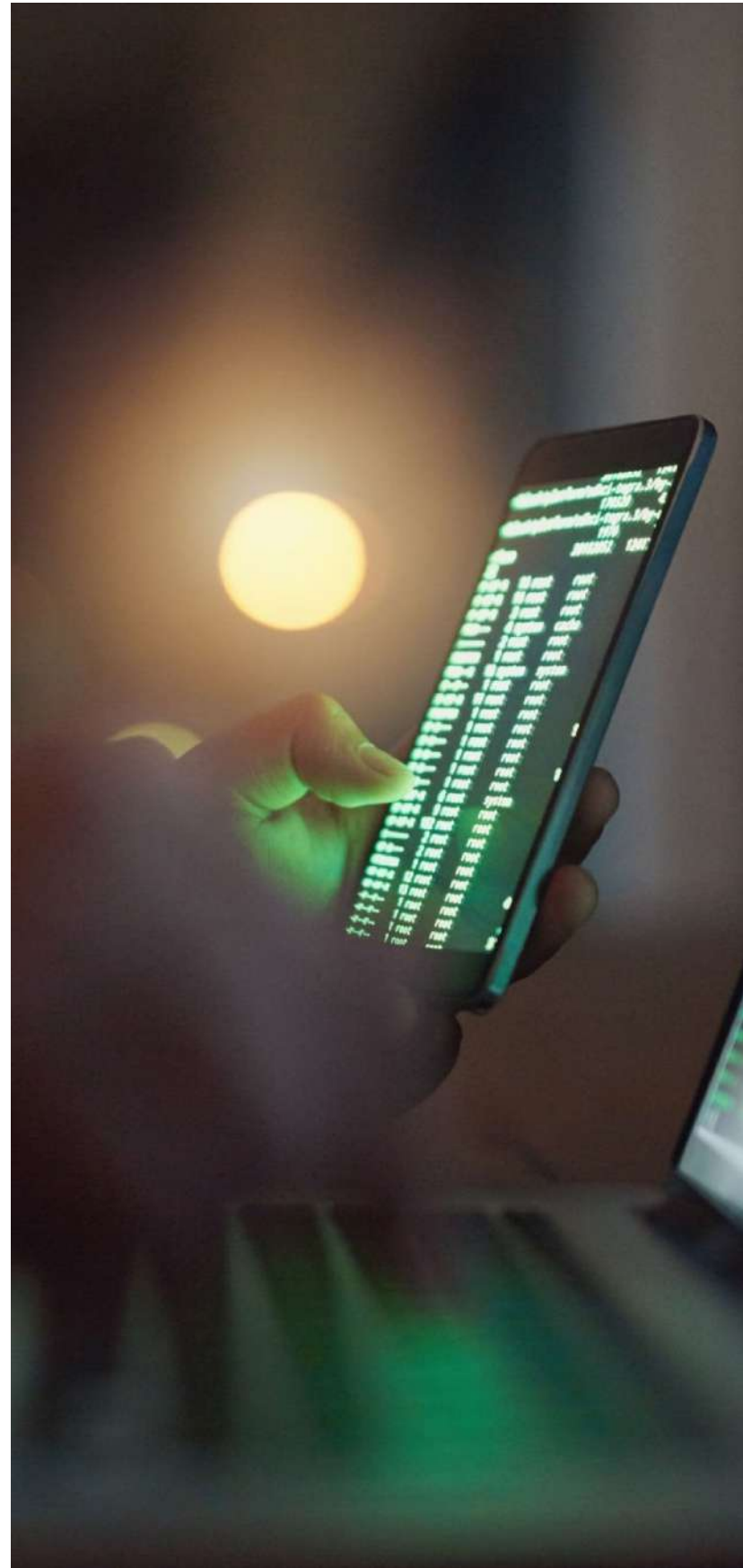
**Muhammed Dishan V**  
MEA21CS055

## Introduction

Phone hacking involves using computer exploits to gain unauthorized access to a mobile device, enabling the analysis of its memory, central processing unit, file system, and processes.

## The Most Common Mobile Hacking Techniques

Mobile hacking is both a fascinating and profitable profession for cybersecurity



enthusiasts and hackers. Given the substantial increase in the number of mobile device users over the previous decade, this makes sense. There are around 3.7 billion mobile phone users worldwide, with over 3 billion using smartphones. Because of the rise in smartphone adoption, which now stands at over 75% in developed economies (mainly western countries) and 52% in developing economies, mobile device security has become a top priority.

In addition to having direct internet connection, the attack surface for mobile devices and endpoints is diversified due to many vulnerabilities associated with mobile devices, just as it is with traditional computing systems (e.g. PCs, servers). The far-reaching consequences of mobile hacking, including reputational harm and financial losses resulting from the theft of private and personally identifiable information, have drastically transformed the cybersecurity environment. Unauthorized access to stored and communication data, recording equipment like microphones and cameras, location data, and peripheral tools like Bluetooth and Wifi, among other things, might be obtained. This section looks at some of the newer methods for extracting personally identifiable information from mobile devices without the users' knowledge. It will be attempted to explain the detection modalities as well as techniques to avoid them.

Hackers aren't reinventing willpower. For mobile device hacking, the same classic or conventional approaches used to target

PCs are being rewritten. Platform differences (Windows/UNIX/Linux for PCs/servers and Android/IOS/Windows for mobile devices) are what have changed.

Here are some of the most typical methods by which hackers get access to your mobile device without your knowledge:

### **Malware:**

Malware remains a powerful technique of gaining access to your mobile device without your authorization, just as it does in the PC and server environment. Malware is introduced into your device and disseminated to other users through the same channels as before, including being tricked into downloading malware-infected files such as gaming, social, or productivity apps, phishing techniques such as email phishing, where tricking links to important resources are sent through email that trigger malware download once clicked, and smishing (sms phishing) attacks where fabricated input forms or malware are sent through SMS. The notorious SkyGoFree, a spyware meant to collect personally identifying information, is one example of known malware for mobile devices. The apps can also gather audio, images, and video from the camera in real time, as well as live position data through GPS, wiretapping phone calls, and event/contextual data collection.

### **Synchronization:**

The notorious SkyGoFree, a spyware meant to collect personally identifying information, is one example of known malware for mobile devices. The apps can also gather audio, images, and video from the camera in real time, as well as live position data through

GPS, wiretapping phone calls, and event/contextual data collection. Some malware (viruses, trojan horses, worms, and so on) may jump to (and potentially from) both ends.

Users should be cautious about who they sync their devices with, as well as peripheral devices they connect to in public locations, since some of them may have been faked or hacked and used to spread malware.

#### **Buffer Overflows:**

This form of attack can jeopardize the integrity of data saved or in transit on a mobile device. When data packet injections are used repeatedly to exceed a temporary storage or memory space in order to overload the devices and render them unusable for legitimate tasks, it might render the device inoperable and allow for remote injection/execution of programmes as well as privilege escalation in order to take control of the devices for illicit or illegal purposes. Unvalidated input vulnerabilities that a hacker may have identified in either an application or the operating system of a device might permit this type of attack.

#### **Denial of Service (DoS) Attacks:**

The purpose of a DoS attack is to flood a mobile device with a huge number of requests in order to overload it, making its resources unavailable or unusable to legitimate users. Most of the time, the hacker must have discovered a vulnerability or loophole of some sort on the device and exploit the same to their advantage not for any real/tangible benefit but to make the device unusable. The aim is to harm the reputation of the phone manufacturer on a large scale, leading to customer dissatisfaction of such a magnitude

that it causes a shift in buyers away from the company.

#### **Old-School Voicemail Attacks:**

Voicemail assaults are a method that dates back to the early days of phreaking and hacking. For customers that have not yet chosen a voicemail PIN, phone providers frequently choose a default PIN code, which is available online. The hacker then dials the target's voicemail, enters the default PIN code, and accesses their voicemail account. The hacker can then gather data from voicemails, obtain illegal access to phone menus, and make unauthorized modifications to voicemail and automated menu-based services.

#### **Bluetooth Techniques:**

Bluetooth hacking is a powerful approach for many mobile device hackers, albeit it is not as often utilized as phishing and malware assaults. Bluejacking is the practice of delivering unwanted messages to Bluetooth-enabled devices such as cell phones, PDAs, and laptop computers over Bluetooth connections. A vCard with a message in the name field (for blue dating or blue chat) is delivered to another Bluetooth-enabled device via the OBEX protocol. Bluesnarfing is getting unauthorized access to data from a wireless device over a Bluetooth connection, which is most often used between Bluetooth-enabled devices such as phones, desktop and laptop computers, and other PDAs. As long as the target's Bluetooth is turned on, the OBEX protocol for Bluetooth business cards (vCard) is susceptible and might be abused by a hacker's device to gain direct access to the target's device without their consent. The lesson here is to always turn off your Bluetooth



when you are not using it.

### **Physical Access to Devices:**

Physical access to a target gadget gives you more control and allows you to do the most damage. Unlike the other tactics, which take some amount of complexity and effort, this attack is more direct with less subtlety. With physical access to the device, attackers can quickly install malware or make covert illicit connections to utilize later. While this type of assault is quite effective, it is the least likely of all due to the work necessary to obtain the target device, unless a close family member or domestic staff member is utilized to assist.

The cornerstone for avoiding the above-mentioned assaults is cybersecurity knowledge and education. Mobile users must be aware of the threat/attack vectors that might aid the perpetration of these types of assaults and protect themselves by adopting a security-conscious mindset. They must be able to spot phishing/smishing communications, guarantee frequent patching of their operating system software and apps for patches released by OEMs and App suppliers, limit physical access to their mobile devices, and switch off file sharing services when not in use, among a slew of other things.

### **Some of mobile hacking tools are the following:**

- Nmap is considered the best hacking tool for port scanning, which is a crucial phase in ethical hacking.
- Nessus.
- Nikto
- Kismet

- NetStumbler
- Acunetix
- Netsparker
- Intrude

### **Ways to Protect Yourself From Hackers**

- Don't access personal or financial data with public Wi-Fi.
- Turn off anything you don't need.
- Choose your apps wisely.
- Use a password, lock code or encryption.
- Be skeptical about links and attachments.
- Trace or erase.

### **Conclusions**

Between attackers and defenders, security is always an arms race. As the market for mobile applications continues to expand, mobile security will present a wider range of challenges. To put it another way, security is frequently a balance of risk and benefit, protection vs convenience. The possible hazards and advantages, as well as their tradeoffs, need additional and deeper examination, according to this school of reasoning. The paper's conclusion is a comprehensive picture of the problem, which looks at the negative events, situations, and circumstances that can lead to asset loss, as well as the remedies that try to eradicate them and offer appropriate and effective security for users.



# PHISHING ATTACK

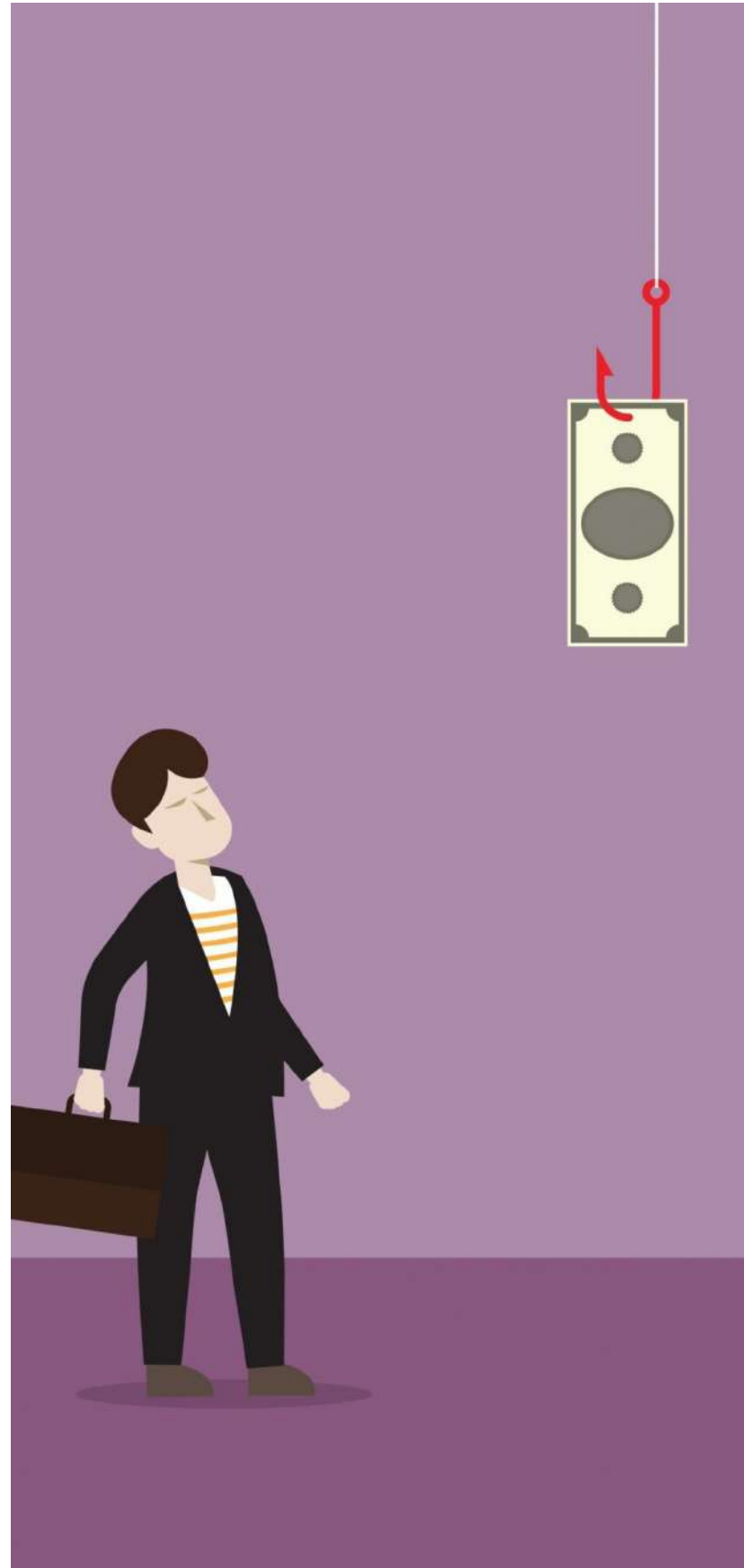
---



**Shafinaz N P**  
MEA21CS081

## Introduction

Why is it crucial to comprehend the risk of phishing? How can phishing assaults be prevented? Many individuals are aware of phishing attempts and the best way to avoid them. The issue of phishing is a serious one that keeps getting worse. According to a Tessian survey from 2021, employees receive 14 phishing emails on average each year. Retail employees, for instance, were particularly negatively impacted, receiving an average of



49. ESET 2021 research found a 7.3% increase in email-based assaults between May and August of that year, the majority of which were phishing attempts. In part because of COVID-19 and supply chain uncertainty, phishing attacks grew by 2 percentage points between 2019 and 2020, according to IBM's 2021 research.

In order to deceive a target into providing sensitive information, such as passwords, personally identifiable information, banking information, and credit card information, an imposter contacts a target by email, phone, or text message. Phishing is the term for this kind of cyber crime. Identity theft and financial loss could arise from using the information to access private accounts. The first phishing case was brought in 2004 against a California kid who constructed a website that looked like "America Online." He was able to obtain sensitive information from users and access credit card credentials in order to withdraw money from their accounts using this false website. Aside from email and internet phishing, fraudsters are continually developing new phishing strategies such as vishing (voice phishing), smishing (SMS phishing), and a variety of other phishing techniques. To gather personal information from users, a variety of methods are employed. The strategies used by cybercriminals are becoming more advanced as technology advances. To avoid falling prey to Internet phishing, consumers should understand how the bad guys operate and be aware of anti-phishing tools.

## **Phishing techniques**

### **Email phishing scams**

Phishing via email is a numbers game. Even if only a tiny number of receivers fall for the scam, an attacker who sends out thousands of bogus communications can obtain valuable information and money. As previously stated, attackers employ a variety of strategies to improve their success rates.

### **Spear phishing**

In contrast to random programme users, spear phishing targets a specific individual or company. It's a more advanced form of phishing that requires in-depth understanding of a firm's power structure.

### **Credits card phishing scams**

It's simple to keep track of your credit card accounts online in our digital age. Many consumers are so busy that they assume every communication they receive from their credit card provider is genuine. A well-designed spoof email or spoof website is the foundation of any successful phishing attempt, which is why it pays to maintain a healthy level of suspicion when reading emails and visiting websites. Financial theft is mainly due to credit card phishing scams.

### **How to prevent phishing?**

Phishing attack protection requires steps be taken by both users and enterprises. For users, vigilance is key. A spoof communication frequently contains small errors that reveal its genuine identity. Users should also consider why they are receiving such an email in the first place.

Enterprises can take a number of steps to protect themselves from phishing and spear phishing attacks:

- The most effective way to combat phishing attempts is two-factor authentication (2FA), which adds an extra layer of verification when logging into key applications. Users require two things in order to use 2FA: something they have, like a smartphone, and something they know, such as a username and password. Even if their credentials are stolen, 2FA prevents employees from accessing the system since it is insufficient.
- In addition to employing 2FA, entities should impose strict password management policies. Employees shouldn't be allowed to use the same password across many applications and should be required to update their passwords on a regular basis.
- By enforcing secure behaviours like not clicking on external email links, educational efforts can help reduce the threat of phishing attempts.

### Top 3 Phishing Simulators

#### Infosec IQ

Infosec IQ by Infosec provides a free Phishing Risk Test that allows you to quickly conduct a simulated phishing campaign and get your organization's phishing rate in less than 24 hours.

#### Gophish

Gophish gets it right as an open-source phishing platform. Most OS systems are supported, installation is as simple as downloading and extracting a ZIP archive, the interface is straightforward and intuitive, and the functions, while restricted, are well-thought-out.

#### LUCY

LUCY is a platform for social engineering that goes beyond phishing. There's also an awareness component with interactive lessons and quizzes.

#### Conclusion

Phishing is a sort of cybersecurity assault in which hostile actors send messages posing as a trusted individual or organization. Phishing communications trick users into doing things like downloading a harmful file, opening a malicious link, or disclosing personal information like login credentials. The most popular sort of social engineering is phishing, which is a broad word for attempts to mislead or deceive computer users. In practically all security events, social engineering is becoming a more common threat vector. Phishing and other social engineering assaults are frequently integrated with additional threats including malware, code injection, and network attacks.





## Design Team



Mr. Asheeque Akthar C



Mr. Mufleh Mohamed P



Mr. Muhammed Muhsin P



Mr. Muhammed Dishan V

**“ Intelligence is the ability to adapt to change ”**

- Stephen Hawking





## **MEA ENGINEERING COLLEGE**

Shihab Thangal Nagar, Vengoor PO,  
Malappuram District, Kerala 679325  
[info@meaec.edu.in](mailto:info@meaec.edu.in) [@www.meaec.edu.in](http://www.meaec.edu.in)