➢ What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

- **Information security** protects the integrity and privacy of data, both in storage and in transit.

- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and

the procedures that determine how and where data may be stored or shared all fall under this umbrella.

- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

➢ Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyber-terrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or

legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured query language) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an

unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

❖ Cyber safety tips - protect yourself against cyber attacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

- ✓ **Update your software and operating system:** This means you benefit from the latest security patches.
- ✓ **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
- ✓ **Use strong passwords:** Ensure your passwords are not easily guessable.
- ✓ **Do not open email attachments from unknown senders:** These could be infected with malware.
- ✓ **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.

✓ **Avoid using unsecure Wi-Fi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

➢ Major Cyber Security Tips

1. Think before You Click

This is one of the most important Cyber Security email tips that you can use and follow regularly to keep your data safe. Stay cautious of the unknown links you receive through emails, messages, or while visiting other web pages that are not secure enough.

Clickjacking is among the most common methods used by hackers to gain access to your personal data. Just because you are capable of clicking these links does not imply that you should because if these links are malicious then, it can cause you to lose hefty amounts and can damage your life in several ways.

Links in mails in the form of password recovery emails, bank statements, etc. are among the most popular methods used by hackers to trick you and gain your personal information. The fake sites connected to these links are too similar to the real ones where the hackers will get you to provide your personal details and gain access to your account using the same.

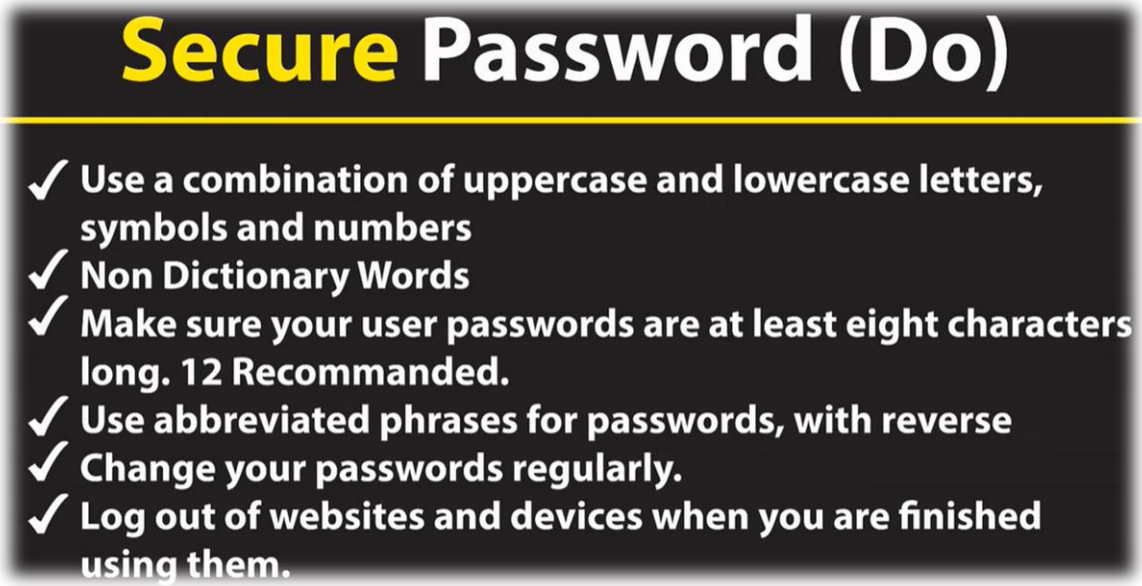
2. **Use Strong and Varied Passwords**

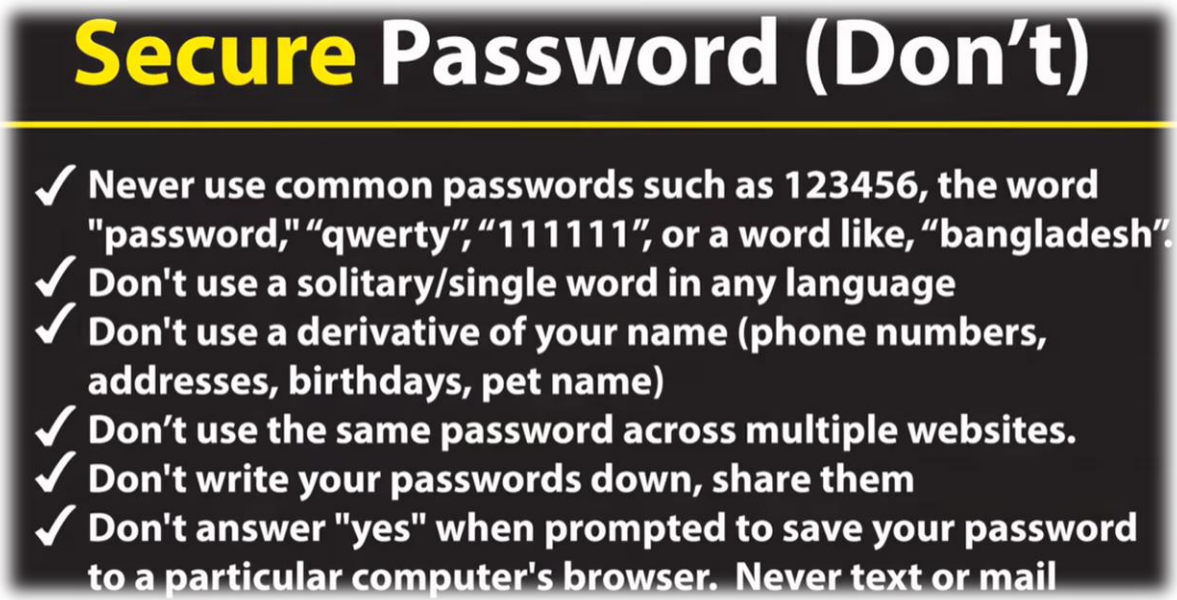
This is another one of the most significant cyber safety tips for users. It may be easy to use and remember the same password across multiple platforms for all your accounts but it makes your account more insecure. You should use distinct passwords for all your different accounts. With this practice, even if a company where you have an account is breached or hackers have gotten access to one of your account credentials, these credentials would not work on other websites.

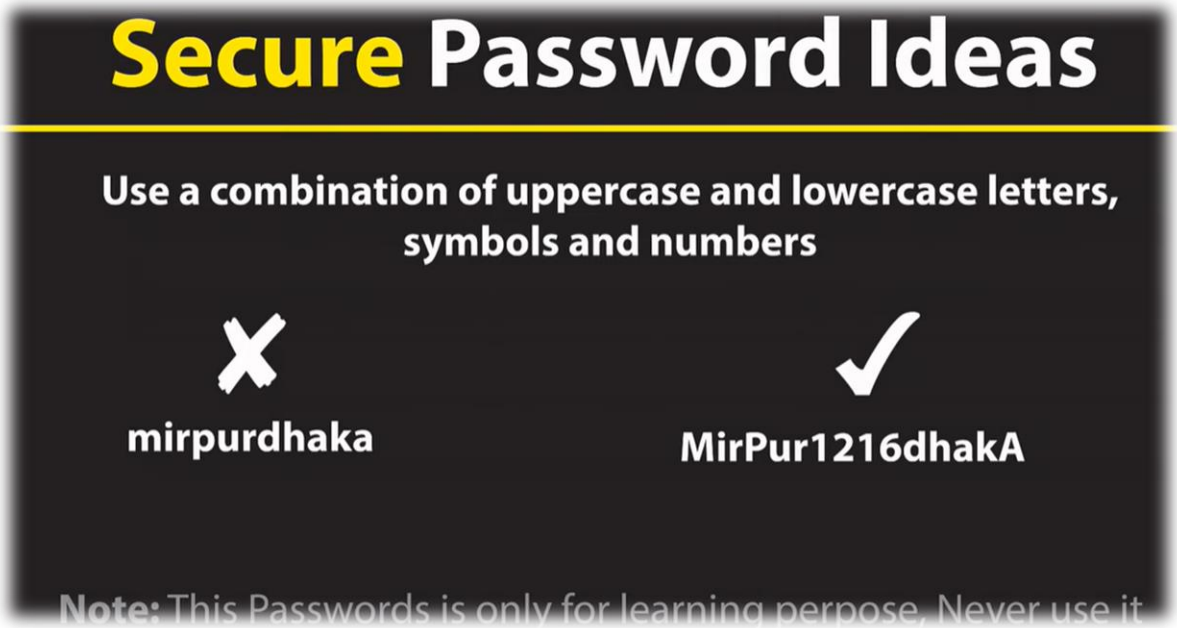
Also, you need to use strong passwords for your accounts as they are important for online security. To make your passwords strong and secure, you can refer to the password policy guidelines of the National Institute of Standards and Technology and consider the following:

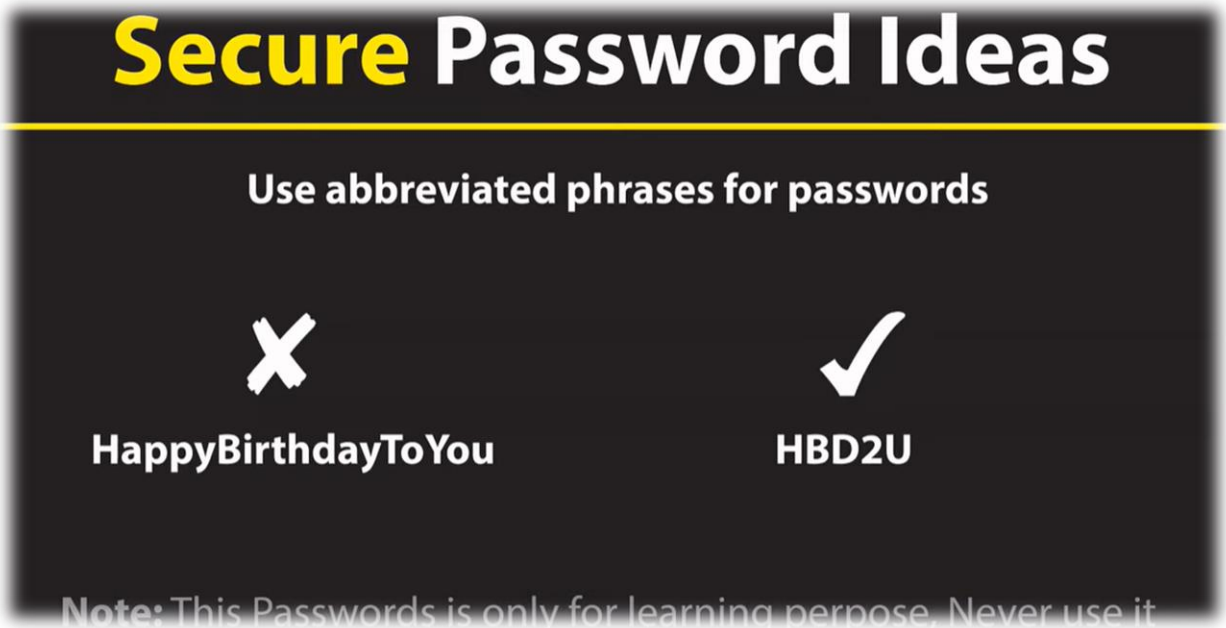
- Use passwords with more than 8 characters and a maximum of 64 characters
- Never make use of the same password twice
- Use at least one uppercase letter, one lowercase letter, one number, and a few symbols other than &, #, _, @, etc.
- Use passwords that are easy to remember and also, do not leave clues in the open or make them available to the public

- Change your password often and reset it.

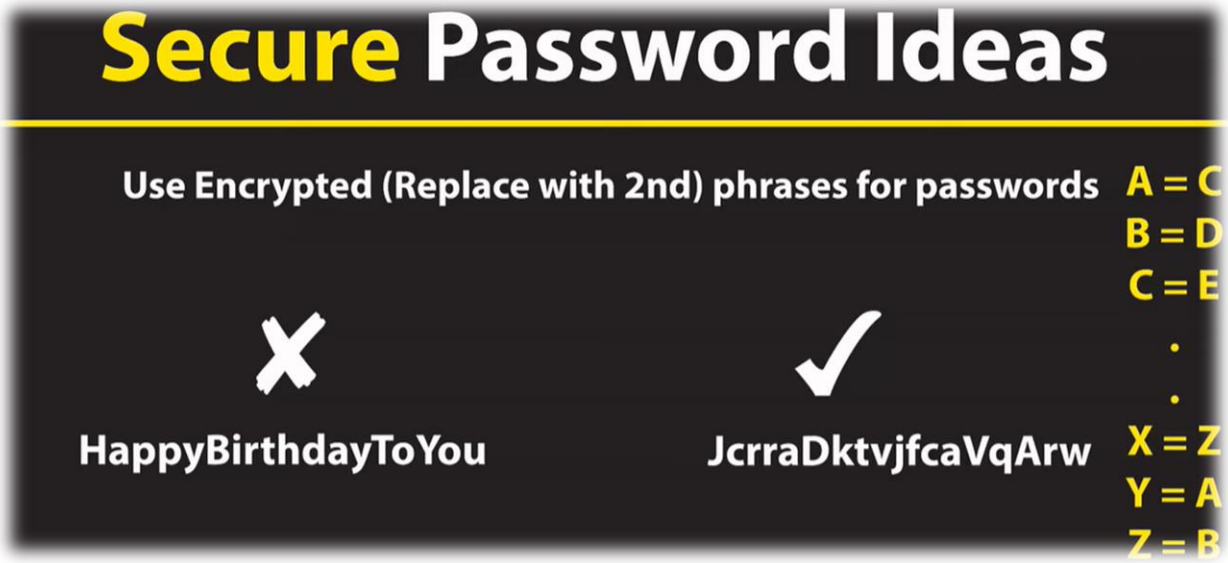



Secure Password (Don't)
✓ Never use common passwords such as 123456, the word "password," "qwerty", "111111", or a word like, "bangladesh".
✓ Don't use a solitary/single word in any language
✓ Don't use a derivative of your name (phone numbers, addresses, birthdays, pet name)
✓ Don't use the same password across multiple websites.
✓ Don't write your passwords down, share them
✓ Don't answer "yes" when prompted to save your password to a particular computer's browser. Never text or mail

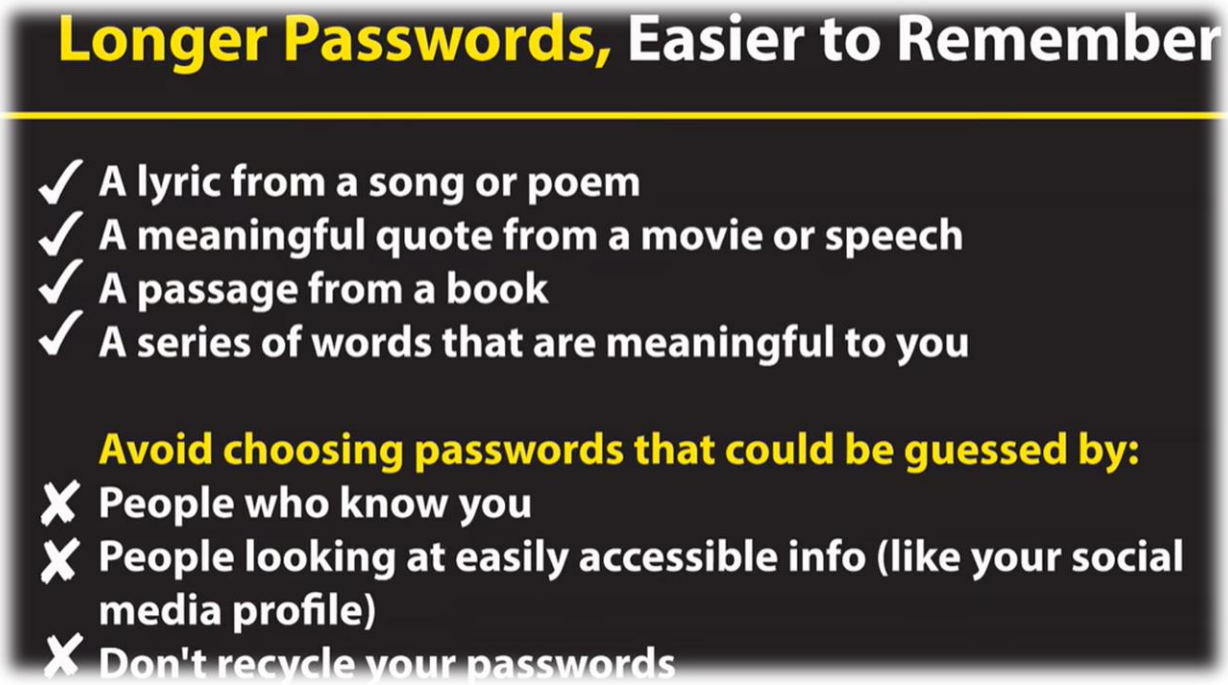

Secure Password Ideas
Use a combination of uppercase and lowercase letters, symbols and numbers
✗
mirpurdhaka
✓
MirPur1216dhakA
Note: This Passwords is only for learning perpose, Never use it

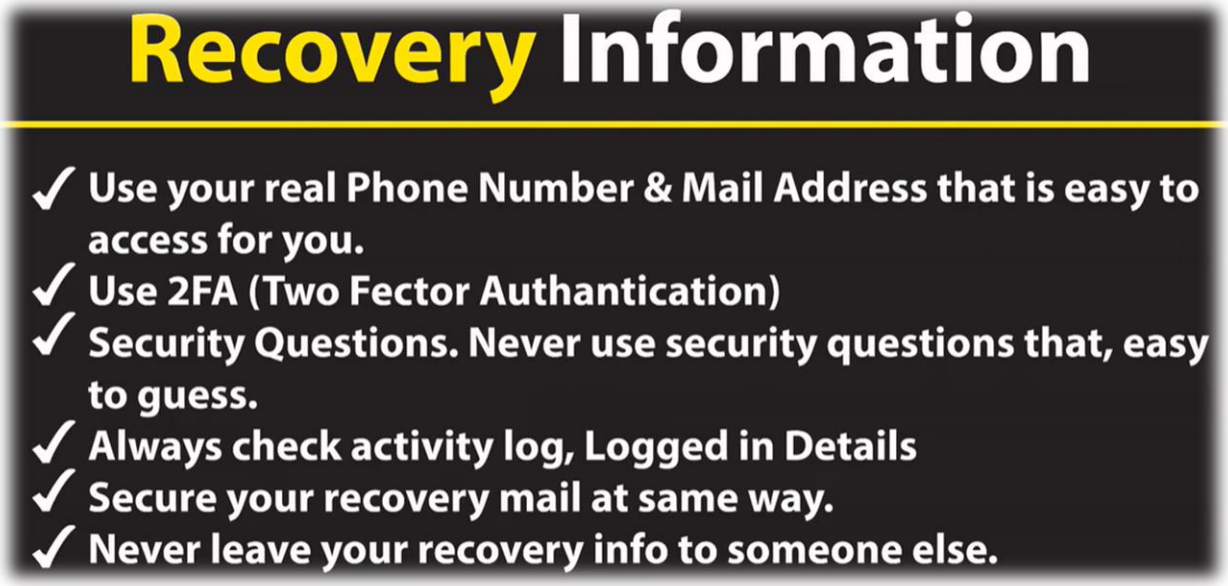

Secure Password Ideas
Use abbreviated phrases for passwords
HappyBirthdayToYou
HBD2U
Note: This Passwords is only for learning perpose. Never use it


Secure Password Ideas
Use Encrypted phrases for passwords
A = 4
E = 3
I = 1
O = 0
S = $
HappyBirthdayToYou
H4ppyB1rthd4yT0Y0u
Note: This Passwords is only for learning perpose. Never use it


Secure Password Ideas
Use Encrypted (Replace with 2nd) phrases for passwords
A = C
B = D
C = E
X = Z
Y = A
Z = B
HappyBirthdayToYou
JcrraDktvjfcaVqArw


Secure Password Ideas
Non Dictionary Words
iamagoodboy
AmiValoChele


Longer Passwords, Easier to Remember
✓ A lyric from a song or poem
✓ A meaningful quote from a movie or speech
✓ A passage from a book
✓ A series of words that are meaningful to you
Avoid choosing passwords that could be guessed by:
✗ People who know you
✗ People looking at easily accessible info (like your social media profile)
✗ Don't recycle your passwords


Recovery Information
✓ Use your real Phone Number & Mail Address that is easy to access for you.
✓ Use 2FA (Two Fector Authantication)
✓ Security Questions. Never use security questions that, easy to guess.
✓ Always check activity log, Logged in Details
✓ Secure your recovery mail at same way.
✓ Never leave your recovery info to someone else.

Password Attacks

Dictionary attack

The hacker is essentially attacking you with a dictionary. A dictionary attack tries a prearranged list of words such as you'd find in a dictionary.

Brute force attack

The attacker automates software to try as many combinations as possible in as quick a time as possible.

In 2012, an industrious hacker unveiled a 25-GPU cluster he had programmed to crack any 8-character Windows password containing uppercase and lowercase letters, numbers, and symbols in less than six hours. It has the ability to try 350 billion guesses per second. Generally, anything under 12 characters is vulnerable to being cracked.

Good News for You, Bad for Attackers

Limit Login Attempts

Limit Login Attempts allows us to track and limit the number of failed login attempts.

Encription such as WPA (Wi-Fi Protected Access)

WEP > WPA > WPA 2 > WPA 3 > WPA 4

WPA3 PSK (Pre Shared Key)

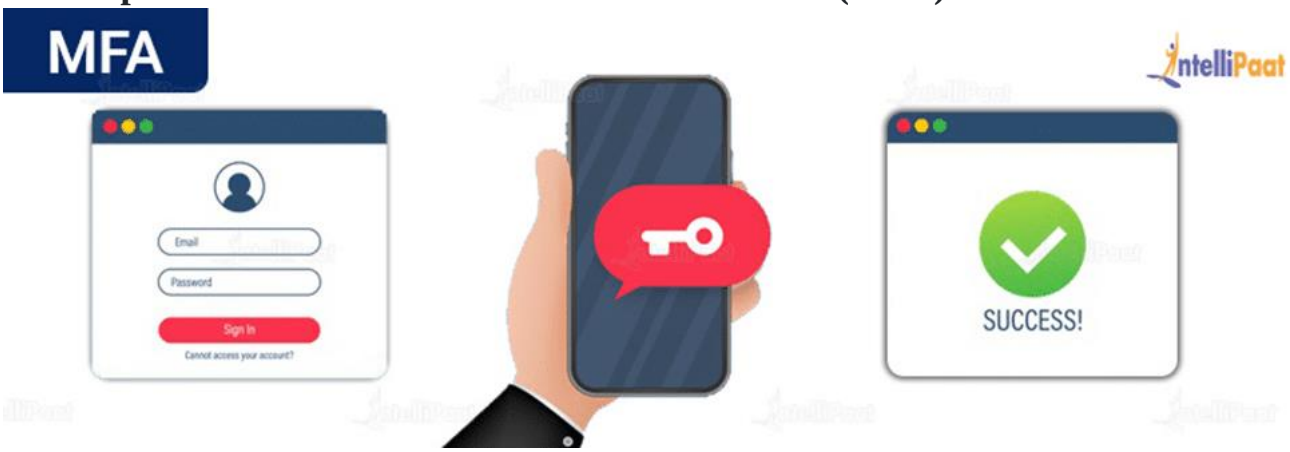
It takes 65,000+ Years to break an 8-digit strong passwords of WPA-2 PSK (Source: IEEE)

3. Use a Password Manager Tool

It may be difficult to remember so many passwords for your various accounts, which is when a password manager comes into the picture. A password manager is a program or software that will help you store and manage all your passwords together. You will be able to access all these passwords using a single ‘master key’ password. This will help you keep these credentials secured and also prevent you from writing down your passwords, which is one of the most unsafe methods of keeping a track of your passwords. It is extremely important in this digital era for you to have cyber safety and security awareness.

It may be difficult to remember so many passwords for your various accounts, which is when a password manager comes into the picture. A password manager is a program or software that will help you store and manage all your passwords together. You will be able to access all these passwords using a single ‘master key’ password. This will help you keep these credentials secured and also prevent you from writing down your passwords, which is one of the most unsafe methods of keeping a track of your passwords. It is extremely important in this digital era for you to have cyber safety and security awareness.

4. Set up Two-factor or Multi-factor Authentication (MFA)



Generally, you require only your user id and your password to sign in to your account but the **MFA** service enables you to add extra security layers to the standard method of using passwords for online verification. With this, you will receive a prompt to add another method of authentication along with the password, like a code, fingerprint, OTP in your phone number or email, etc. With this method, you will be required to enter more than two credentials while logging in, keeping your account more secure by making it more difficult for hackers to access your data. This is another one of the most significant Cyber Security measures that you must take.

5. Check CERT-In Updates on a Regular Basis

CERT-It stands for Computer Emergency Readiness Team- India. It came into operation in January 2004 and falls in the constituency of the Indian Cyber community. CERT-In basically serves as the national agency to perform various functions in the Cyber Security domain such as cyber security incident forecast and alerts, emergency response actions for tackling cyber security events, etc. Hence, regular checking of CERT-In updates is very important to deal with cyber emergencies.

6. Keep Your Systems Updated

Another one of the most crucial cyber safety tips is that you must keep all your browsers, software, and operating systems up-to-date. This is especially one of the most important Cyber Security tips for the workplace and also for users. If your organization firewalls for security purposes, you must update that as well. The older your system and its configurations are, the longer the hackers have to find and exploit all the weaknesses. Updating them will prevent attackers from exploiting them for enough time until new updates.

7. Use Firewalls and Anti-viruses

Hackers can attack your systems and networks through various methods, such as malware, viruses, phishing attacks, trojans, spyware, etc., to gain access to your data. With the help of anti-virus software and firewalls, your system will be capable of defending itself against these attacks. You need to ensure that your firewall or the software that you are using is updated regularly and prevents such cyber threats before they occur.

You can use antivirus software like McAfee, TOTAL AV, Norton, etc., and firewalls, such as NGFW, **NAT** firewalls, etc. In order to keep your data protected

from all possible threats, it is important for you as a user or an employee to have Cyber Security awareness.

8. Avoid Online use of Debit Cards

One of the most useful Cyber Security measures that you can take is regarding online transactions and payments. When you purchase services or products online, try to avoid paying through debit cards or any other payment method that is connected to your bank account directly. Rather, you can make use of applications like PayPal or credit cards, which will provide more protection to your bank accounts.

9. Avoid Unfamiliar Websites

When you come across new sites shared by your friends or even strangers online, be cautious of visiting them because some of them may contain drive-by download attacks that can attack your system data.

This type of attack does not require you to click on anything in order to get the computer infected. It attacks your system by injecting malicious code as soon as you click on the link of the website. So, it is recommended to steer clear of such websites and visit only well-established websites that you are familiar with.

10. Avoid Useless Downloads

Downloads are among the top tricks used by attackers and hackers to gain access to your networks and systems. You should limit your downloads to save your systems and data from any such threats. You must avoid downloading unnecessary software and browser extensions. In the case of an organization, employees should be given authorization before they download any software using the internet.

One of the Cyber Security measures that you can take to download safely is to choose the process of custom installation while installing anything and go through each of

the steps carefully. During the installation process, if you receive pop-ups for any extensions or add-ons, you must decline them.

11. Stay Cautious on Social Media

Yes, in this modern, digital era, it has become easy for us to reconnect and get in touch with our friends and family through various social media platforms over the internet, such as Facebook, WhatsApp, LinkedIn, etc. However, you need to be careful of whatever you share with them online. Hackers can gain a lot of information from your social media pages and profiles. So, ensure that you share a limited amount of information on the internet since it can easily be accessed by hackers.

14. Make Your Data Backup Regularly

Backups are nothing but a copy of the files or network's data for the purpose of restoration in case of damage or loss. Cyber-attacks may lead to data loss and file damage. In certain situations, there is no guarantee that the attackers will return the stolen data even after paying the ransom. Hence, it is always advisable to create data backup to mitigate the loss from cyberattacks.

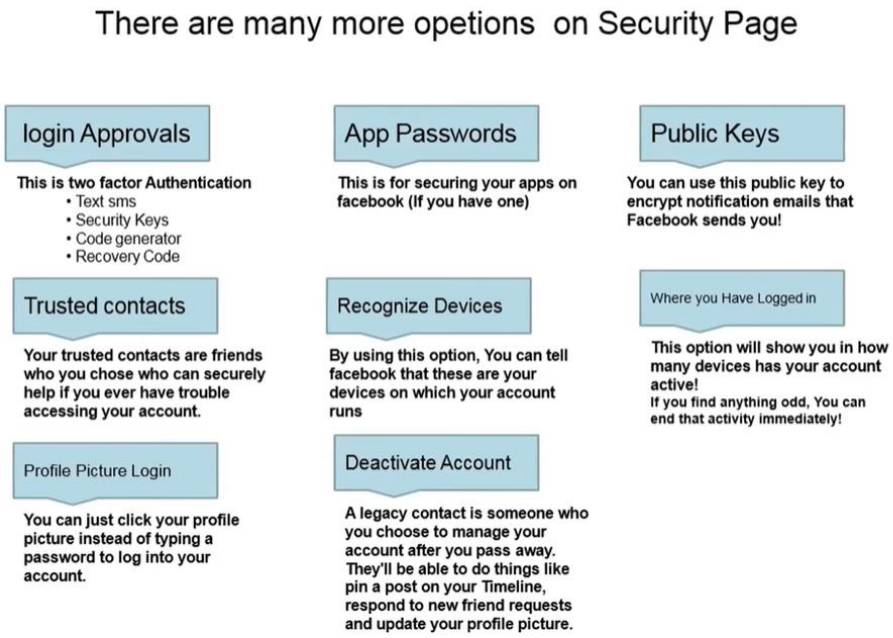
14. Don't Use Public WiFi without a VPN

If you are using public WiFi, make sure that you use a Virtual Private Network (VPN) along with it. VPN allows your device to be secured as it encrypts the traffic between the server and your device. This increases the difficulty of

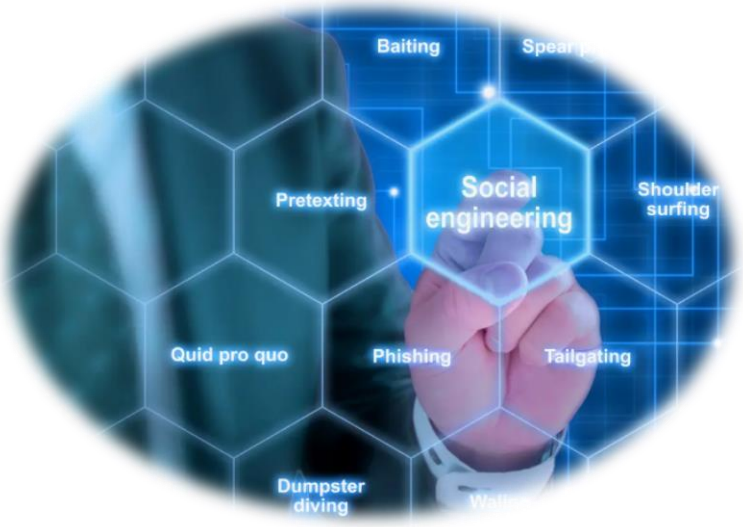
hackers when they try to access your personal data by hacking into your device. If you do not have a VPN on your device, you should use a mobile network or other connections to use the internet.

15. Secure Your Data

It is important for you to have Cyber Security awareness so that you are capable of securing your data from external threats and hackers. In this section, you have come across some of the most helpful tips that can help you keep your personal data and systems safe from any such attacks. To learn more about the attacks and how you can prevent them from occurring, you should apply for our Cyber Security program which will help you gain in-depth knowledge of this IT domain.



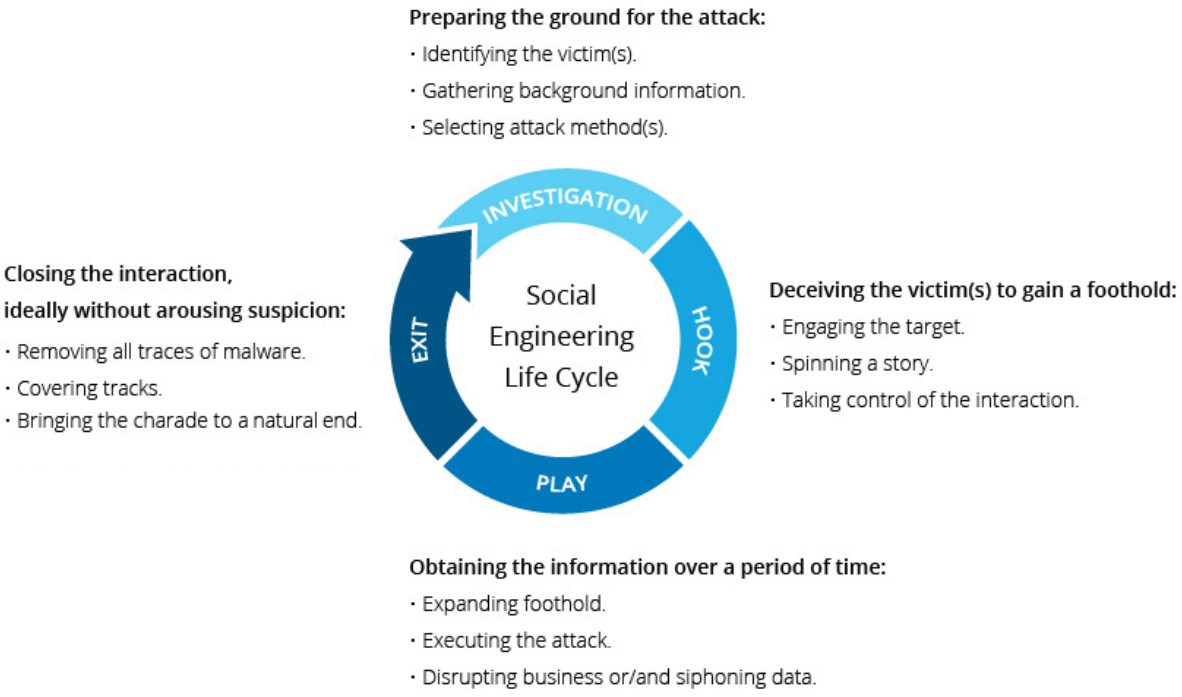
➢ Social Engineering Attacks



What is social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.



Social Engineering Attack Lifecycle

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Social engineering attack techniques

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the most common forms of digital social engineering assaults.

Baiting:

1. Definition of Baiting Attacks:

- Baiting attacks involve the use of false promises or enticing offers to exploit human curiosity or greed.

- They aim to trick victims into revealing personal information or infecting their systems with malware.

2. Physical Baiting Techniques:

- Attackers distribute malware-infected physical media, such as flash drives, in high-traffic or conspicuous areas.
- The bait is designed to appear authentic, often masquerading as company-related documents like payroll lists.
- When victims pick up the bait and insert it into a computer, it leads to automatic installation of malware on the system.

3. Online Baiting Techniques:

- Online baiting involves the use of enticing ads that direct users to malicious websites or encourage them to download malware-infected applications.
- These ads often exploit popular topics, trends, or clickbait tactics to attract users' attention.

4. Protective Measures against Baiting Attacks:

- Educate employees and users about the risks associated with unsolicited physical media or suspicious online ads.
- Implement strict security policies, such as prohibiting the use of unauthorized external devices on company computers.
- Utilize reliable antivirus and anti-malware software to detect and prevent malware installations.
- Foster a culture of cybersecurity awareness, encouraging users to verify the authenticity of any unexpected or enticing offers before taking action.

Scareware:

1. Definition and Characteristics:

- Scareware is a deceptive tactic used by cybercriminals to trick users into believing their computer is infected with malware.
- It involves bombarding victims with false alarms and fictitious threats, often through popup banners or spam emails.
- Scareware may offer to install supposed security tools (which are often malware-infected) or direct users to malicious websites.

2. Common Scareware Tactics:

- Popup Banners: Legitimate-looking popups on web browsers with alarming messages about potential malware infections.
- Spam Emails: Deceptive emails that distribute fake warnings and offer worthless or harmful services to users.
- Social Engineering: Scareware relies on psychological manipulation to create a sense of urgency and fear.

3. Impacts and Risks:

- Financial Loss: Users may purchase useless or harmful software or services, wasting money.
- Malware Infections: Scareware can actually introduce malware to a victim's system, leading to data breaches and privacy issues.
- Loss of Trust: Victims may become skeptical of legitimate security warnings, making them more vulnerable to real threats.

4. Preventive Measures:

- Educate Users: Teach individuals to be cautious when encountering unsolicited popups or emails with alarming messages.
- Use Reliable Security Software: Encourage the use of trusted antivirus and anti-malware tools to prevent and detect real threats.
- Regular Software Updates: Keep software and operating systems up to date to minimize vulnerabilities that scareware can exploit.

Pretexting:

1. Definition of Pretexting:

- Pretexting is a deceptive social engineering technique used by attackers to obtain sensitive information by impersonating trusted individuals or authorities.

2. Attack Process:

- The attacker initiates the scam by establishing trust with the victim, often impersonating co-workers, police, bank officials, or other figures with authority.
- The pretexter asks seemingly legitimate questions to confirm the victim's identity, gradually extracting personal data.
- Information gathered includes social security numbers, addresses, phone records, financial data, and even physical security details.

3. Targets and Consequences:

- Pretexting attacks can target individuals, employees, or even organizations.
- Consequences can range from identity theft and financial fraud to breaches of sensitive business data, potentially leading to financial losses and reputational damage.

4. Prevention and Awareness:

- To prevent pretexting attacks, individuals and organizations should be cautious about sharing personal or sensitive information without proper verification.
- Employee training and awareness programs can help recognize and respond to pretexting attempts.
- Implementing strict data protection and access control measures can reduce the risk of falling victim to pretexting attacks.

Phishing Attacks:

Definition:

- Phishing attacks are deceptive attempts to impersonate legitimate entities or organizations, primarily using email communication to trick individuals into revealing sensitive information.

Attack Process:

- Unsolicited and fraudulent emails with enticing subject lines or urgent calls to action.
- Use of familiar branding and logos to appear legitimate.
- Links to malicious websites or attachments that can install malware or steal information.

Prevention and Awareness:

- Educate individuals to scrutinize emails, check sender addresses, and verify the legitimacy of requests.
- Implement robust email filtering and spam detection systems.
- Use multi-factor authentication for sensitive accounts.

Spear Phishing Attacks:

Definition:

- Spear phishing attacks are highly targeted and customized forms of phishing that focus on specific individuals or organizations, using personalized messages.

Attack Process:

- Extensive research on the target, often utilizing social media profiles.
- Personalized emails that reference specific information or events, creating a sense of authenticity.
- Crafting messages to appear as if they come from a trusted source within the organization.

Prevention and Awareness:

- Train employees to be cautious about sharing sensitive information, even if the request appears legitimate.
- Raise awareness about online privacy and the risks of oversharing on social media.
- Encourage reporting of suspicious emails or activities.

Common Red Flags:

1. Generic Greetings:

   - Many phishing emails use generic greetings like "Dear User" instead of personal salutations.

2. Urgent Calls to Action:

   - Phishing emails often create a sense of urgency to prompt immediate action.

3. Misspelled URLs or Email Addresses:

   - Carefully examine email addresses and URLs for any misspelled or suspicious elements.

4. Unsolicited Attachments or Links:

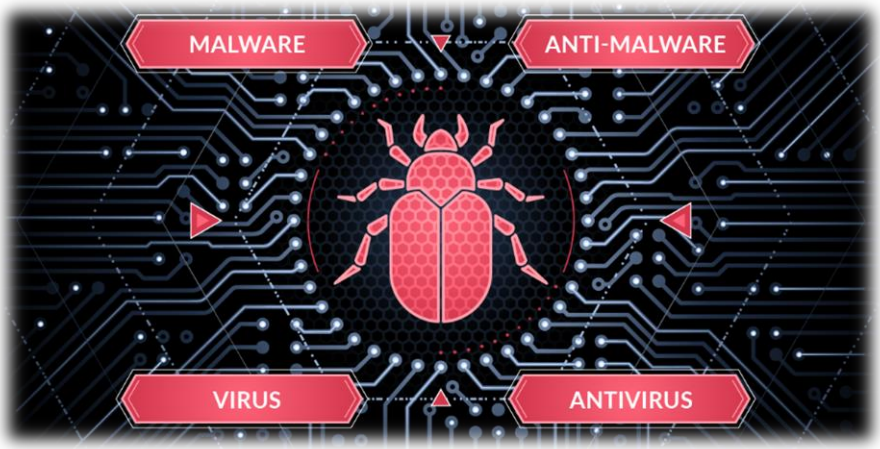
- Be cautious when receiving unsolicited files or links, even if they appear to be from trusted sources.

S. No.	PHISHING	SPEAR PHISHING
1.	Phishing attack is done for a wide range of people.	Spear phishing is done for specific person or organization.
2.	Its objective is to steal sensitive data like bank card details from maximum people.	Its objective is to steal sensitive data from a large company regarding stacks etc.
3.	It is an automated attack.	While it is a manual attack.
4.	The targets selected in phishing are very random.	While target is specific in spear phishing.
5.	This is broad and less sophisticated.	While this is more sophisticated.
6.	The target has high volume- hundreds or thousands of recipients of spam.	The target has low volume- sent to one individual or a small group of individuals, such as the accounts department.
7.	It is mostly done for money.	While it is done to ruin an organization.
8.	It is impersonal, such as sending generic greetings.	It is extremely customized since attackers would research their targets to create a convincing email.
9.	Phishing includes cyber criminals or professional hackers.	While spear phishing attackers are business oriented malicious code distributor

Real-World Examples:

1. Target Data Breach (2013)

2. Google Docs Phishing Scam (2017)



What is antivirus?

Antivirus is a software program designed to prevent, detect, scan, and delete viruses from your device. Most antivirus software runs in the background while you're online and provides real-time protection against harmful cyberattacks. Some antivirus programs include additional security solutions like a firewall or ad blockers.

The purpose of antivirus is to guard against computer viruses and remove any threats detected. Your antivirus should keep your device clean and malware-free.

Different antivirus software works in various ways:

- Behavior-based detection looks at the intention of an object. If it's unauthorized, the antivirus shows the file as having malicious intent.
- Heuristic-based detection looks for previously known issues and flags them as suspicious.
- Signature-based detection will tag an object for future reference after analyzing it for specific patterns.
- Application whitelisting only allows files and programs to run that are known to be good and can help protect endpoints like your smartphone, tablet, or other connected devices.

What is anti-malware?

Anti-malware software protects data from malware, or malicious software and files. The software scans a device to prevent and remove malware. It is developed to safeguard your computer system from various types of malware, like newer Trojans, adware, ransomware, spyware, keyloggers, phishing, and worms.

Anti-malware software protects your device from newer, more sophisticated cybersecurity threats, like the ones in the wild. In-the-wild threats are viruses that spread on real-world devices, not just in test environments. These threats have been discovered on machines being used for real-world purposes.

Anti-malware uses three techniques to detect malware issues. These methods are behavior-based, signature-based, and sandboxing.

- Behavior-based detection looks for suspect processes that match malicious behaviors.
- Signature-based detection uses a unique digital footprint of malware that has already been discovered and looks for them on your device.
- Sandboxing runs the suspect object in a virtual environment and analyzes the behavior, isolating it from other files for safety.

What's the difference between antivirus and anti-malware?

Antivirus programs protect against more established threats, like the traditional worms, viruses, and Trojans. Anti-malware specializes in newer exploits, like polymorphic malware and zero-day malware.

Antivirus programs are good at protecting against more predictable, dangerous malware. Anti-malware protects more of the current, yet still dangerous, online threats. Sometimes anti-malware updates the detection rules faster than antivirus, so it may detect malware faster against newer threats if you're browsing the internet frequently.

Still, antivirus offers better protection against malware you could obtain from traditional sources. If you get a dangerous email attachment or link, a good antivirus is your best friend. Antivirus is also a strong protector against viruses generally obtained through external devices like USBs.

Polymorphic viruses can change form to avoid detection, replicating themselves into different shapes. Since these threats can change form, it's nearly impossible for antivirus programs to catch or prevent them.

Zero-day malware gets pushed out before software companies have the time to release a patch for the problem. These threats are aptly named because there is zero time to develop a patch for them. That delay leaves a wide open window of time for virus vulnerability

Which one should I use?

Since technology is ever-evolving, it may be hard for one program to catch every virus or malware threat. We think your best bet is to get both. If you have a solid antivirus catching all the traditional threats, and anti-malware guarding against the newer ones, you'll have much less to worry about.

You don't always have to buy two different programs to accomplish this. A software program like Malwarebytes Premium combines both types of security to offer dual protection. If you decide to get two products, make sure they will work while running together. Some products cannot run at the same time.

If you're on a budget and can only afford to purchase one, we recommend an antivirus program because they're great for casting a wide net of protection against known malware attacks. Most antivirus programs also offer malware detection and malware removal tools.

If you're more concerned with being proactive against new threats and want tools that can destroy activated malware, shopping for good anti-malware tools may be the best option. Anti-malware may offer you a comprehensive solution to maintain online security against all the new viral threats.

Best antivirus and anti-malware software

You can go with a solid antivirus like **AVG**, a budget-friendly software, or **Malwarebytes**, which has been a trusted name for many years.

Keep in mind that the best antivirus software doesn't have to be the most expensive. Programs like **TotalAV**, which is our budget antivirus pick, and **Avast's free antivirus** still offer excellent protection. These programs won't interrupt your workflow and have been around for years, so they're some of the more trusted products. They also won't break the bank!

You could opt for a program like **Adaware** or **Spybot Search & Destroy** if you want to check out anti-malware tools. These are two of the popular programs often purchased. Ad-Aware comes with a webcam blocker, so hackers can't watch you while you're online. Spybot comes with several different features, like rootkit scans and antispyware tools.

The key differences between antivirus and anti-malware software:

1. Scope:

Antivirus: Antivirus software primarily focuses on detecting and preventing traditional viruses. These are malicious programs that replicate themselves and can infect other files and systems. Antivirus software is designed to identify and neutralize viruses.

Anti-Malware: Anti-malware software has a broader scope. It encompasses a variety of malicious software, not just viruses. It is designed to detect and remove a wide range of threats, including viruses, Trojans, spyware, adware, worms, rootkits, and more.

2. Types of Threats:

Antivirus: Antivirus software is specifically designed to combat viruses. It may not be as effective at dealing with other types of malware.

Anti-Malware: Anti-malware software is versatile and capable of addressing various types of malware, making it a more comprehensive solution.

3. Detection Methods:

Antivirus: Antivirus programs primarily use signature-based detection. They compare files and programs on your computer with a database of known virus signatures. If there's a match, the antivirus program recognizes the threat.

Anti-Malware: Anti-malware software employs a variety of detection methods, including signature-based scanning, behavioral analysis, heuristics, and anomaly detection. This multifaceted approach allows it to detect a broader range of threats.

4. Real-Time Protection:

Antivirus: Antivirus software often focuses on real-time protection against known viruses. It may not be as proactive against emerging or unknown threats.

Anti-Malware: Anti-malware tools are often more proactive in detecting new and emerging threats by analyzing behaviors and characteristics that might be associated with malware.

5. System Performance:

Antivirus: Antivirus software is usually optimized for faster scanning and may have a lighter impact on system resources, making it suitable for everyday use.

Anti-Malware: Anti-malware programs may be more comprehensive but could be resource-intensive, impacting system performance, especially during scans.

6. Usage Scenario:

Antivirus: Antivirus software is suitable for users primarily concerned about protecting their systems from virus infections. It is often used as a core security component in many devices.

Anti-Malware: Anti-malware software is more versatile and is suitable for users who want comprehensive protection against a wide range of threats, not limited to just viruses.

7. Multilayered Protection:

Antivirus: Antivirus can be part of a multilayered security strategy, working alongside other security tools to provide comprehensive protection.

Anti-Malware: Anti-malware software often incorporates multiple layers of protection within a single program, making it a comprehensive security solution on its own.

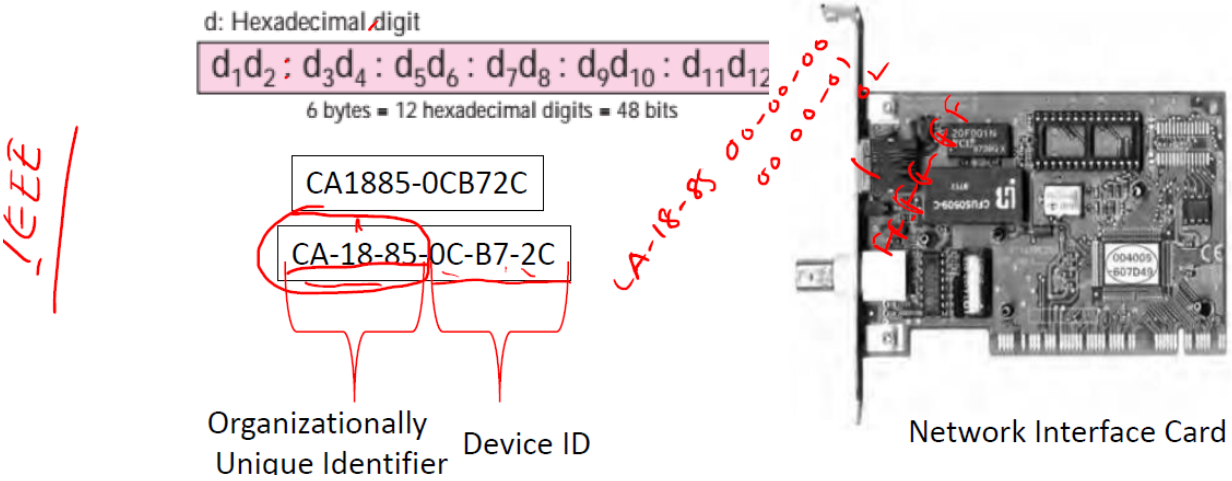
Classification of Address

- Address
  - Physical Address
  - Logical Address
  - Port Address

Physical Address

- the address of a node as defined by its LAN
- The lowest-level address
- The size and format of these addresses vary depending on the network
  - Ethernet uses 6 bytes address (imprinted on Network Interface Card (NIC))

- 6 byte address is also called *Medium Access Control (MAC)* address
- No two NICs ever share the same MAC address
- Either imprinted on the surface or burnt into a ROM chip



What's Your MAC Address?

You can readily determine your MAC address on a modern computer from the command line.

1. In Windows Vista/7, click Start, enter **cmd** in the Start Search text box, and press the ENTER key to get to a command prompt.
2. In Windows 8, simply type **cmd** at the Start screen and press ENTER when the Command Prompt option appears on the right.
3. At the command prompt, type the command **ipconfig /all** and press the ENTER key.

Logical Address

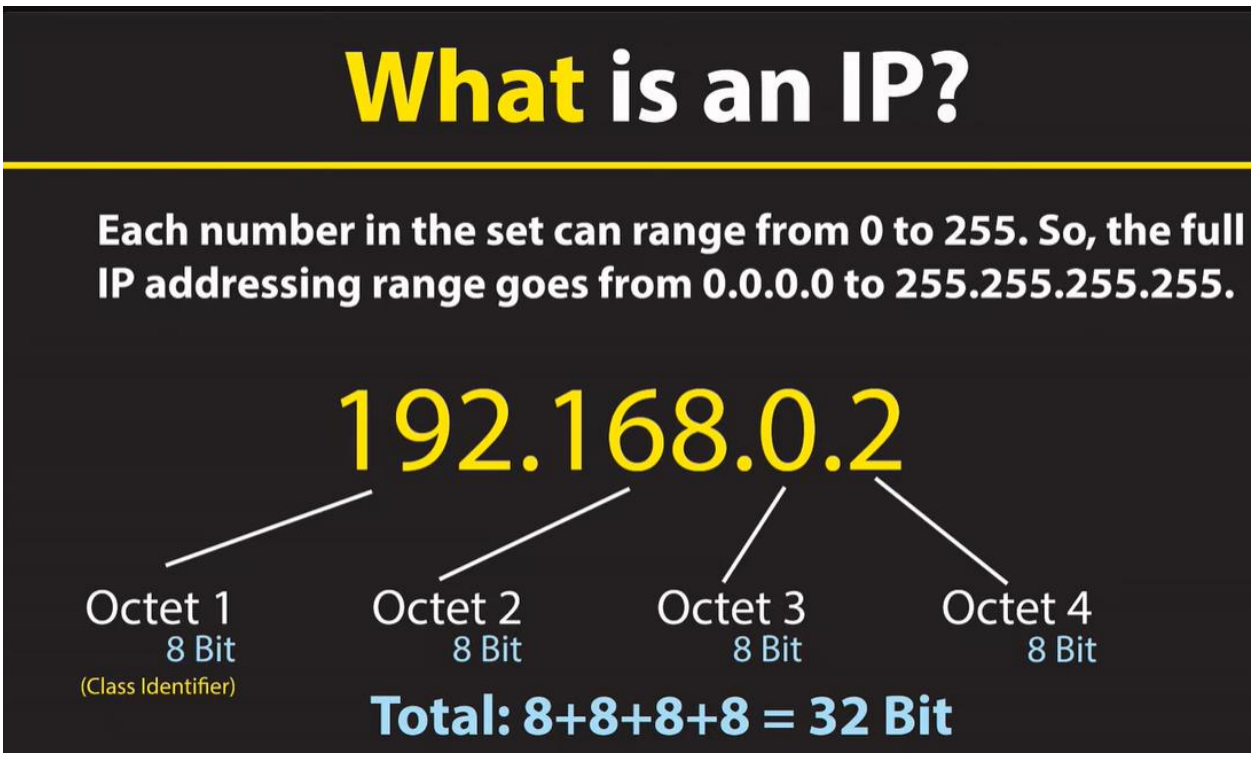
- Physical address is not suitable for internetwork as different networks can have different address formats
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network
- Can be changed depending on the network
- No two publicly addressed and visible hosts on the Internet can have the same logical address (widely known as Internet Protocol (IP) address.
- 32-bits length

IP Address

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol,"

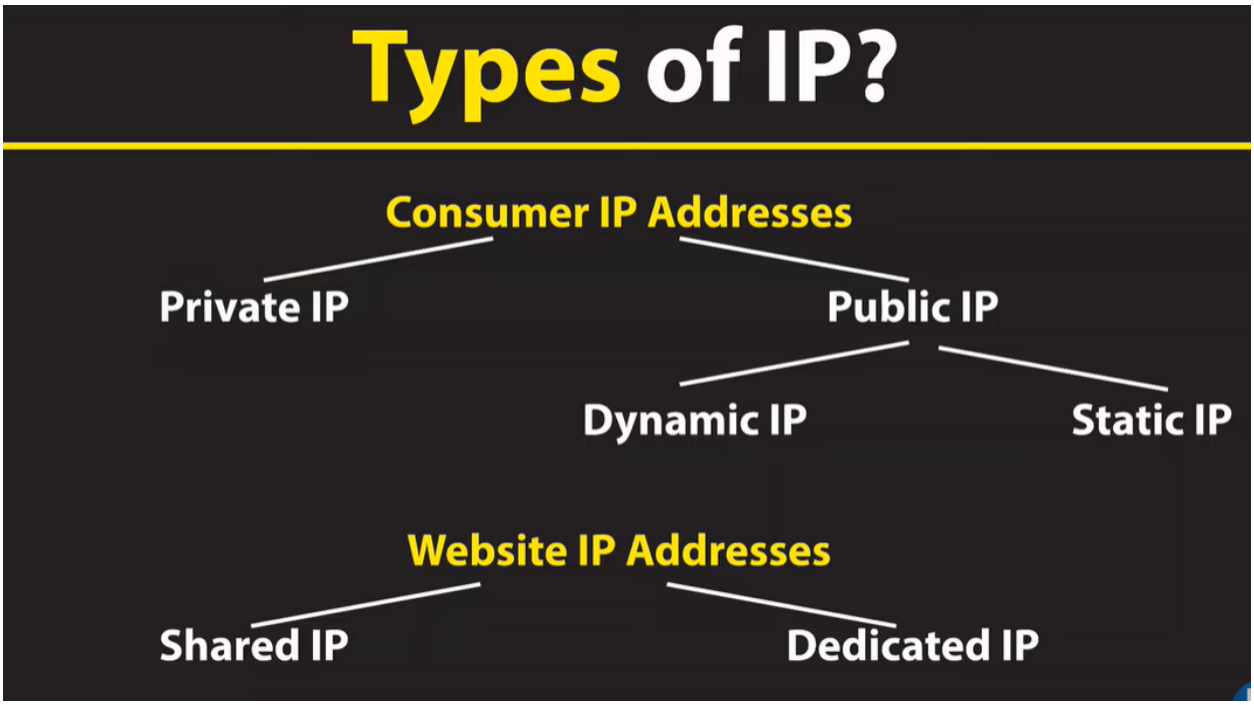
192.168.0.1 192.168.0.2 192.168.0.3

IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication.



What is an IP Class?

Class	Value	Example	SM (Bit)
A	0-127	80.123.22.12	8
B	128-191	145.22.13.223	16
C	192-223	210.112.123.9	24
D	224-239	225.212.0.90	-
E	240-255	245.12.35.22	-


Types of IP?
Consumer IP Addresses
Private IP
Public IP
Dynamic IP
Static IP
Website IP Addresses
Shared IP
Dedicated IP


IP address security threats
Online stalking
Downloading illegal content using your IP address
Tracking down your location
Directly attacking your network
Hacking into your device
How to protect and hide your IP address
Using a proxy server
Using a virtual private network (VPN)

Binary-to-Decimal Conversion

For addressing, we require
to convert a 8-bits binary to decimal
To convert a decimal number of up to 255 to binary number

Digit	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1
Position of digit, i	8	7	6	5	4	3	2	1
Contribution of the digit, 2^{i-1}	2^{8-1}	2^{7-1}	2^{6-1}	2^{5-1}	2^{4-1}	2^{3-1}	2^{2-1}	2^{1-1}
Decimal contribution	128	64	32	16	8	4	2	1

$2^{8-1} = 128$ $2^{5-1} = 2^4 = 16$

1 0 0 1 1 0 0 1

if $x_i = 1$, *add* 2^{i-1} *to the sum* *for* $\forall i$

Digits	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**
Position	8	7	6	5	4	3	2	1
Contribution	128			16	8			1

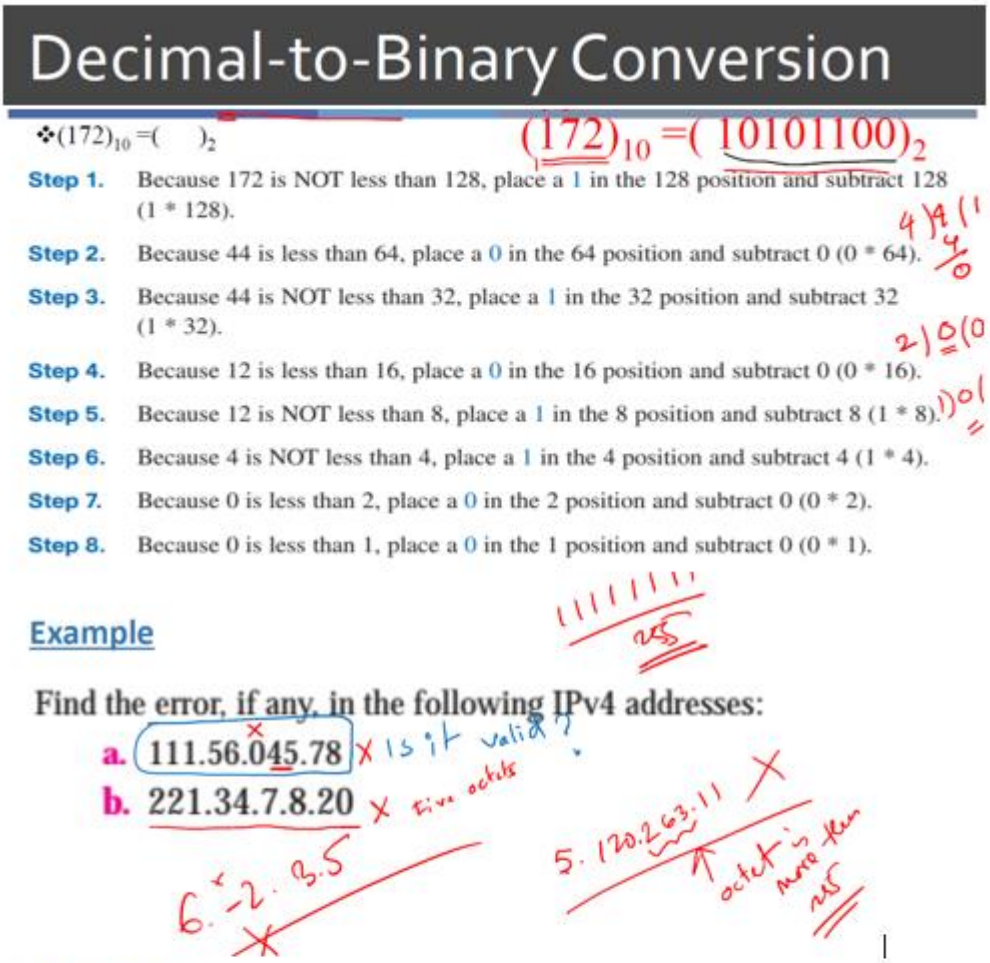
128+16+8+1=153

$(10011001)_2=(153)_{10}$

	0	**1**	**0**	**0**	**1**	**1**	**0**	**1**
		64			8	4		1
Digits	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**
Position	8	7	6	5	4	3	2	1
Contribution		64		8	8	4		1

64+8+4+1=77

$(01001101)_2=(77)_{10}$



Decimal-to-Binary Conversion

❖$(172)_{10}$ =($)_2$ $(172)_{10}$ =($10101100)_2$

Step 1. Because 172 is NOT less than 128, place a 1 in the 128 position and subtract 128 (1 * 128).

Step 2. Because 44 is less than 64, place a 0 in the 64 position and subtract 0 (0 * 64).

Step 3. Because 44 is NOT less than 32, place a 1 in the 32 position and subtract 32 (1 * 32).

Step 4. Because 12 is less than 16, place a 0 in the 16 position and subtract 0 (0 * 16).

Step 5. Because 12 is NOT less than 8, place a 1 in the 8 position and subtract 8 (1 * 8).

Step 6. Because 4 is NOT less than 4, place a 1 in the 4 position and subtract 4 (1 * 4).

Step 7. Because 0 is less than 2, place a 0 in the 2 position and subtract 0 (0 * 2).

Step 8. Because 0 is less than 1, place a 0 in the 1 position and subtract 0 (0 * 1).

Example

Find the error, if any, in the following IPv4 addresses:

a. 111.56.045.78 X Is it valid?

b. 221.34.7.8.20 X Five octets

6. -2. 3.5 X

5. 120.263.11 X octet is more than 255

Example

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Example

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

How It Works Today

Today, your IP address is configured and created by that very same TCP/IP protocol system—so that whenever you're on a computer and have access to a network (at

home, at work, at an airport or hotel), you and your computer can join in on the online fun.

Your home has a street number; your computer (and your smartphone, your smart thermostat, and anything else that connects to the internet) has an internet number.

Do you want to know something extra cool? Every website has a unique IP address, but when you connect to the site, you only see the domain name. For example, when you go to amazon.com, you don't see the string of numbers; you just see "amazon.com." But if Amazon didn't have an IP address, you couldn't connect with their website, and they couldn't tell you what they have for sale.

So now that we've covered what IP addresses are and why they're needed, we'll dive deeper into everything you need to know about your IP address. You'll wow your tech professional friends with your comprehensive knowledge. Let's take a look at the definitions and examples of different types of IP addresses.

Types of IP Addresses

The IPv4

The most common type of IP address is known as IPv4, for "IP version 4." Here's an example of what an IPv4 address might look like:

24.156.99.202

An IPv4 address consists of four numbers, each of which contains 1-3 digits, with a single dot (.) separating each number. Each of the four numbers can range from 0 to 225. This group of numbers creates a unique address to let worldwide users send and retrieve data over internet connections.

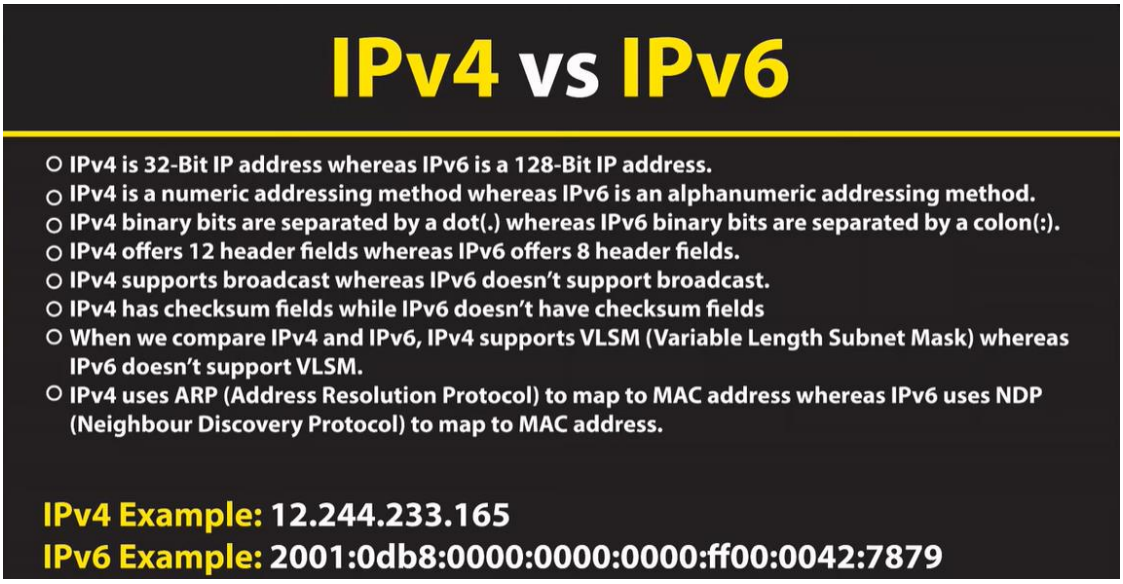
Goodbye IPv4, Hello IPv6

IPv4 supports a maximum of approximately 4.3 billion unique IP addresses. IPv6 supports, in theory, a much higher maximum number: **340,282,366,920,938,463,463,374,607,431,768,211,456.**

If your eyes glazed over when reading that number, rest assured there's no chance of ever running out again.

An IPv6 address consists of eight groups of four hexadecimal digits. Here's an example IPv6 address:

2001:0db8:85a3:0000:0000:8a2e:0370:7334



IP Address Facts

These quick facts about Internet Protocol and IP addresses will help you learn more about what they are and how they work:

1. IP is actually networking software. It comes with your computer and it makes it possible for you to interact with the internet.

2. IP is actually part of a longer abbreviation, TCP/IP. That stands for Transmission Control Protocol/Internet Protocol. (We'll call it IP for short.)
3. The TCP/IP Protocols are actually a set (or stack) of protocols that work in sequence. Think of the set as a team of robot-soldiers who receive, handle, and disburse data.
4. IP is the universal language of the internet (so to speak): All IP networking software is identical throughout the world; that's why a computer in China can communicate with a computer in Canada.
5. IP is versatile. Any computer, phone, or printer on a network has IP software (and therefore an IP address).
6. The Internet Protocol is at the heart of network connectivity. It is also where IP address activity gets processed.
7. Any device on a network has and needs an IP Address. That address is a set of numbers and dots. Find out what your IP address is.
8. Computers identify websites by their IP addresses. Fortunately for us, another protocol, called Domain Name System, or DNS, translates a URL like whatismyipaddress.com into the hexadecimal IP address the software needs.

Reference:

[1] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] https://intellipaat.com/blog/cyber-security-tips-best-practices/

[3] https://www.aura.com/learn/types-of-social-engineering-attacks

[4] https://www.geeksforgeeks.org/difference-between-phishing-and-spear-phishing/

[5] https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[6] https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[7] https://whatismyipaddress.com/ip-facts

[8] https://whatismyipaddress.com/ip-address

[9] https://www.investopedia.com/terms/i/ip-address.asp

[10] https://www.imperva.com/learn/application-security/social-engineering-attack/

[11]

[12]

[13]

[14]

[15]

[16]