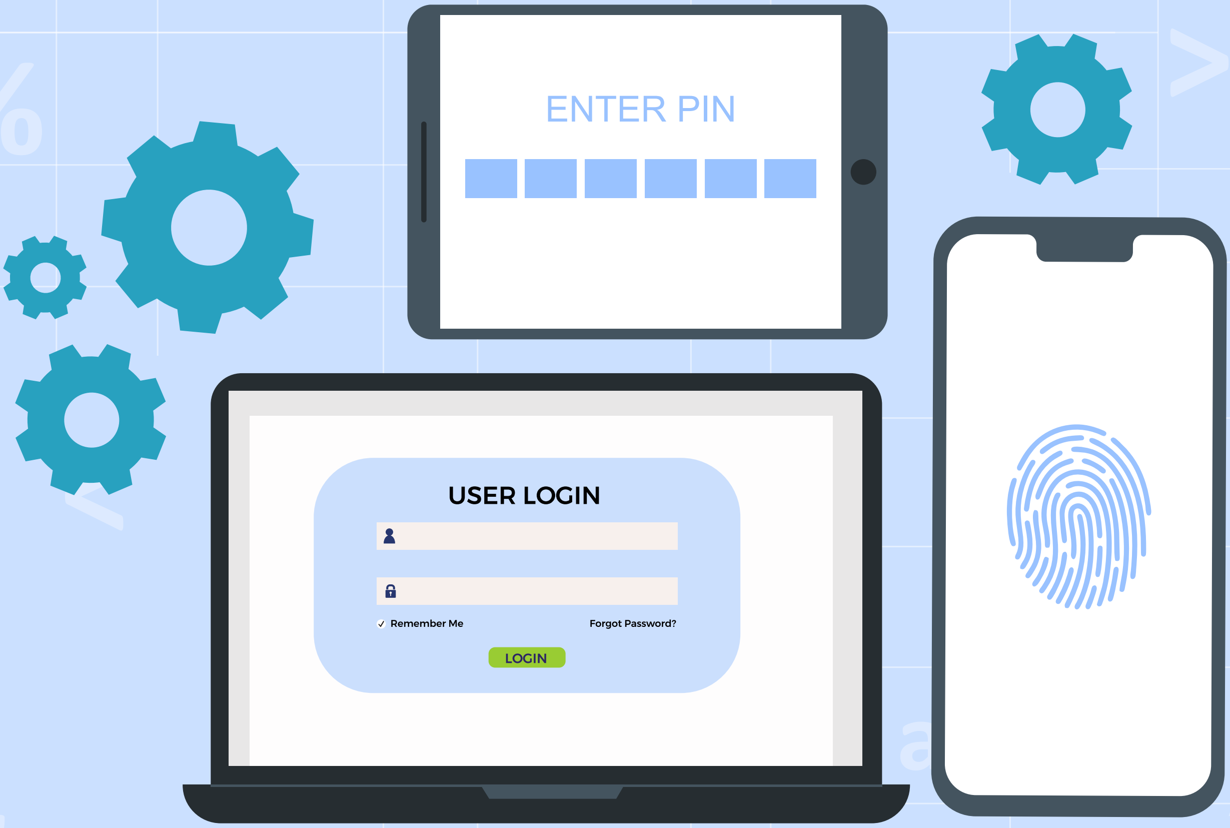
इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

www.isea.gov.in

PASSWORD SECURITY

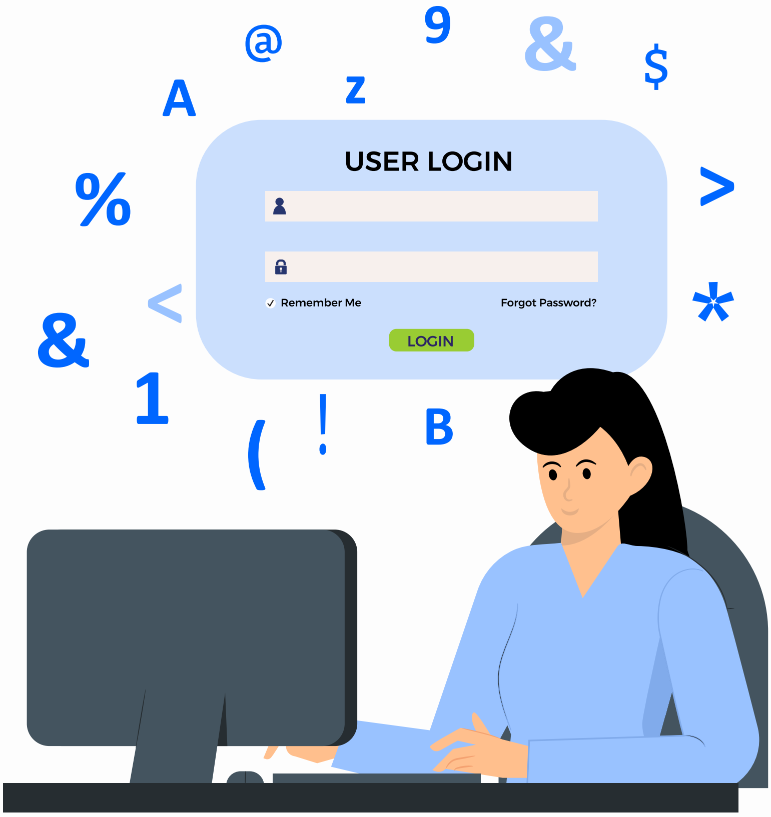


Password Security

What is Password?

A password **is typically a string of characters** that a user must provide in order to confirm their identity and gain access to a system or service. Passwords are a common method of authentication, which are used to verify the identity of a user.

Passwords are commonly used to protect accounts, files, and other sensitive information. It is important to use strong and unique passwords, and to avoid reusing the same password across multiple accounts.



Uses of passwords:

Authentication

A password reliably authenticates or validates the identity of the owner/user of the device.

Access

A password ensures access to the device by the actual user.

Security

A password ensures security to the data, network and information by restricting the user access.

Importance of password while making digital/online transactions:

- Represents and authorizes the identity of the user of a system
- Helps users protect personal information data from unauthorized access
- Acts like a barrier between the user and personal information

To increase the security of passwords and its management, it is important to follow some of the steps while creating passwords, such as:

1 Using a long and complex password that is difficult to guess or crack. This typically means using a mix of upper- and lower-case letters, numbers, and special characters.

iL0v3Bl@Ckc0L0r

2 Avoiding using easily guessed information, such as your name, address, or phone number, in your password.

pinky123 🚫

3 Using different passwords for different accounts, so that a compromise of one password does not give an attacker access to multiple accounts.

4 Updating passwords regularly, especially if there is any suspicion that a password may have been compromised.

5 Two-factor authentication (2FA) can be another great step to secure the password, which it adds extra verification.

Advantages of securing password

There are several advantages to having strong password security:

Protection of sensitive information: Passwords help to protect sensitive information, such as personal information, financial information, and confidential business data, from unauthorized access.

Protection of online accounts: Passwords help to protect online accounts, such as email accounts and social media accounts, from unauthorized access. This can prevent identity theft and other forms of online fraud.

Protection of networks and systems:
Passwords can be used to protect networks and systems from unauthorized access, which can prevent unauthorized users from gaining access to sensitive information or causing damage to the network or system.

Compliance with regulations:
Strong password security is often a requirement under various regulations, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS), which organizations must comply with in order to avoid penalties.

Better security for multi-user and shared systems:
Multiple user accounts can have different levels of access, by giving different passwords this way you can have better control of what information or action each user can do in a specific system.

Possible Vulnerabilities

There are several possible vulnerabilities of relying solely on password-based security:

- Passwords can be easily forgotten, resulting in locked accounts and lost productivity.
- Passwords can be guessed or cracked through various means, such as brute-force attacks or dictionary attacks.
- Passwords could be shared with others and might be misused.
- Users may note down their passwords in a book which can be accessed and viewed by others.
- Passwords can be stolen through phishing scams or other types of social engineering attacks.
- Passwords can be shared or reused, creating a single point of failure if the password is compromised.
- Passwords can also be stored in plain text in the servers, and if the servers are compromised, the passwords are also compromised.
- If a user is using weak and easily guessable passwords, it increases the vulnerability for account getting hacked.

As a security measure **Multi-factor authentication, password managers, and other forms of authentication** can be used in conjunction with passwords to mitigate these risks.

Potential Threats:

There are several threats to password security, including:

Phishing:
Hackers can use phishing emails and websites to trick users into giving away their passwords.

Malware:
Malicious software, such as keyloggers, can be installed on a user's device to record and steal their passwords.

Brute force attacks:
Hackers can use automated software to try a large number of different passwords until they find the correct one.

Dictionary attacks:
Similar to a brute force attack, a dictionary attack uses a pre-compiled list of commonly-used words and phrases to try and guess a password.

Social engineering:
Hackers can use social engineering tactics to trick users into revealing their passwords.

Database breaches:
Hackers can steal passwords by gaining unauthorized access to a company's database where user's passwords are stored.

Weak and reused passwords:
using weak and commonly used passwords and using the same password for multiple accounts can make it easier for hackers to guess or steal your passwords.

Unsecured networks:
Using unsecured networks such as public Wi-Fi to access sensitive information can make it easier for hackers to intercept your passwords.

It's important to be aware of these threats and to take steps to protect your passwords, such as using a strong and unique passwords, using a password manager, enabling two-factor authentication, and being cautious when clicking on links or entering personal information online.

Risks involved with stolen passwords:

There are several possible risks involved with stolen passwords. These include:

Unauthorized access to sensitive information:
If a hacker obtains your password, they can use it to access your email, bank accounts, and other sensitive information.

Identity theft:
A stolen password can be used to steal your identity and commit fraud.

Financial loss:
Hackers can use stolen passwords to make unauthorized purchases or transfer money from your accounts.

Damage to reputation:
A stolen password can be used to send spam or offensive messages from your account, damaging your reputation.

Compliance and legal risk:
Some industries such as healthcare, finance, and government have strict regulations regarding data protection. A stolen password can result in non-compliance with these regulations and legal action.

It is important to use different passwords for multiple accounts and make it a habit to change the passwords to be changed on regular basis from time to time.

Techniques used by hackers/crackers to retrieve your passwords

As passwords are key to repository of valuable information/ data stored in a device, it is not surprising that there is a great possibility of the same getting cracked or hacked. It is one of the most common security threat/attack that is used to by fraudsters to bypass or exploit the authentication of user accounts or to get access to device.

Let us discuss some of the common techniques used by fraudsters for getting hold of user's password/s-

1 Shoulder Surfing

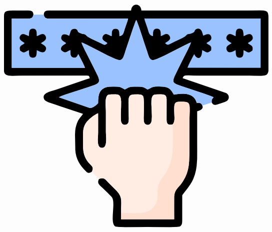
One way of stealing the password is by standing behind a user and overlooking their password while they are typing it. It can happen even by listening to your conversation or while the user is giving away/sharing sensitive information like password over a phone. Shoulder surfing is easily done in crowded places.

Few tips to avoid threats from shoulder surfing.

- Be aware of Shoulder Surfers at public places while you are entering your passwords into the login accounts.
- Do not reveal your usernames and passwords to strangers.
- Cover the keyboard with your hand or something else to prevent view to a stranger.

2 Brute-force attacks

When hackers try to steal the password by guessing and using all possible combinations with the help of personal information of an individual it is known as bruteforce attack. In this attack the hacker tries breaking the password using person's name, pet name (nick name), numbers (date of birth, phone numbers), school name...etc., The hackers use fast processors and some software tools to crack the password.



Few tips to avoid threats from Brute force attack.

- You should not use a password that represents your personal information like nicknames, phone numbers, date of birth etc.
- Making passwords more complex increases the difficulty of attacks that rely on brute force or educated guessing.

3 Dictionary attacks

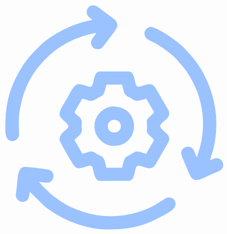
Hackers also try with all possible dictionary words to crack your password with the help of some software tools. This is called a "Dictionary attack".

Few tips to avoid threats from Dictionary attack.

- You should not use dictionary words (like animal, plants, birds or meanings) while creating the passwords for login accounts.
- Better to lock the account or increase the delay between login attempts when there have been repeated failures

4 Password recovery/reset systems

The systems that are in place to allow a legitimate user to recover or change a password when required, can be misused from the password hackers/fraudsters. The fraudster may persuade the authentication system to either mail it to them or change it to something of their choice. Next level of verification mechanism in such cases can serve as protection only if the answers are not very obvious.



ew tips to avoid threats from password recovery/reset systems

- Use information that is not in social media for recovery of password
- Activate two factor/multi factor authentication

5 Phishing/Keylogger/sniffer

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, to trick the recipient of mail/message to reveal sensitive information liker user name, password, PIN etc.,. Phishing is typically carried out by e-mail or instant message spoofing and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

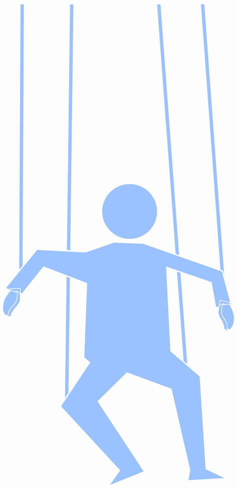
The fraudsters may also make use of a software or hardware by installing it on the user's computer to capture passwords typed on a computer is a 'Keylogger'. Some of these softwares or hardwares can intercept or sniff and log traffic that passes over a computer network and so are called sniffer.

Few tips to avoid threats from Phishing/Keylogger/sniffer

- Be watchful of emails asking for login information
- Double check the URLs before logging into accounts
- Install reliable antivirus software and firewall on the device
- Use a VPN when connecting to public Wi-Fi networks
- Use encryption while sharing data
- Regularly update all software and devices with latest security patches

6 Social Engineering

The simplest way to discover someone's password is to make them tell you their password. Sharing the passwords with the unknown persons (strangers) can lead to misuse of information, access to private account/device and can lead loss of personal information/sensitive data. This can be done by persuading them to type it into a website you control (phishing).



Few tips to avoid threats social engineering

- Beware of any pretext by caller or stranger requesting for sensitive information like PIN, password etc.,
- You must not share passwords with unknown persons (strangers) through email or SMS or any other means.
- Never click on suspicious links or believe any calls or posts for free offers/lottery/gifts etc., asking you for personal information

7 Using weak/easy Passwords

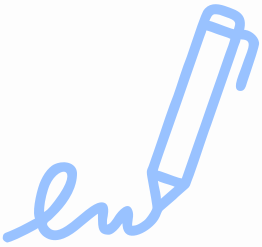
Weak and blank passwords are one of the easiest ways to attackers to crack into your system. Cyber criminals can use the same techniques used to guess the answers to secret questions can also be used to guess passwords. Anything based on something your friends will know, or that is available from a website, is a very poor choice as a password.

Always you need to "Use Strong Passwords"

8 Writing your passwords on the papers or storing it

The strangers search for the papers or the disk for passwords where they have been written.

- You should not write the passwords on the paper or on any disk drive to store it.
- Do not select 'Yes' when applications ask you if you want them to remember your passwords for you.



9 Rainbow table attack

Rainbow tables aren't as colourful as their name may imply but, for a hacker, your password could well be at the end of it. This table contains hashes of all possible password combinations for any given hashing algorithm. Rainbow tables are attractive as it reduces the time needed to crack a password hash to simply just looking something up in a list. However, rainbow tables are huge, unwieldy things.

10 Credential stuffing

This is an automated method, where attackers use pre-computed lists of credentials obtained from past breaches, and test them on other websites. If the same username and password is being used on multiple sites, this can result in multiple accounts getting compromised.

The best way to prevent such attacks is to use unique, complex and long passwords, regularly update the passwords and enable two factor authentication wherever possible.

Also keep an eye on any suspicious activity on the accounts, and act fast in case of any unusual access or login.

Best Practices

There are several best practices that can be followed to secure passwords and keep them safe from being cracked:

Use unique, complex, and long passwords:
A strong password should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information such as your name, birthdate, or common words.

Use a password manager:
A password manager can generate and store complex, unique passwords for you. It can also help you keep track of your passwords and automatically log you into your accounts.

Enable two-factor authentication (2FA):
Two-factor authentication adds an extra layer of security by requiring a second form of verification in addition to your password. This can be a fingerprint, a security code sent to your phone, or a security key.

Regularly update your passwords:
Passwords should be updated regularly, especially if there is a suspicion of them being compromised or if there's been a data breach of one of the sites you use.

Do not reuse passwords:
Reusing the same password across multiple accounts makes it easier for attackers to gain access to multiple accounts if they are able to crack one password.

Educate yourself and your colleagues about phishing scams and social engineering:
Phishing and social engineering attacks are common ways for attackers to steal passwords. Being aware of these types of attacks and knowing how to spot them can help protect your passwords.

Avoid writing down or sharing passwords:
Keep your passwords private, do not share your passwords with anyone, even your colleagues, and do not write them down in a place where they can be easily found.

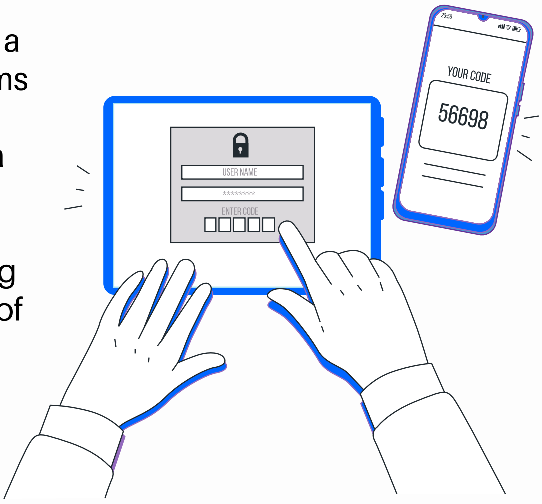
Be wary of public Wi-Fi:
Public Wi-Fi networks can be easily compromised by attackers. Avoid entering sensitive information, such as passwords, while connected to a public Wi-Fi network.

Monitor your accounts:
Regularly check your account activity and look for any suspicious login attempts or changes made to your account information.

By following these best practices, you can significantly reduce the risk of your passwords being compromised. And also using a combination of these practices makes it much harder for an attacker to gain access to your account.

What is Two-factor authentication (2FA)?

Two-factor authentication (**2FA**) is a method of confirming a user's identity by requiring them to present two different forms of evidence, typically something they know (such as a password) and something they have (such as a phone with a code sent via text message).



Multi-factor authentication (**MFA**) is a method of confirming a user's identity by requiring them to present multiple forms of evidence. Typically, MFA requires at least three forms of evidence, which are grouped into categories such as something the user knows (e.g. password), something the user has (e.g. mobile phone), and something the user is (e.g. fingerprint or facial recognition).

By requiring multiple forms of evidence, MFA makes it much more difficult for an attacker to gain unauthorized access, even if they have obtained two forms of evidence (e.g. password and mobile phone).

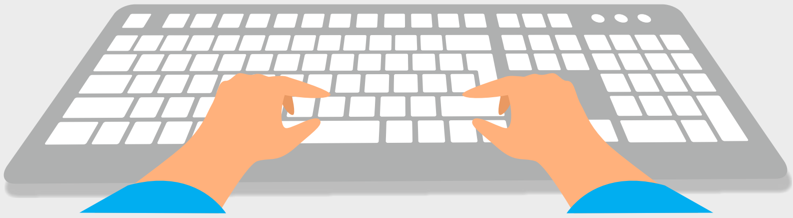
This helps to ensure that the person attempting to gain access to an account is actually the account holder himself, rather attacker.

MFA can be implemented in a variety of ways, including via text message, phone call, email, mobile app, or biometric authentication. Multi-factor authentication (MFA) is indeed considered to be more secure than two-factor authentication because it involves more forms of evidence and therefore makes it more difficult for an attacker to gain unauthorized access.

PASSWORD

is a key element in
Protecting your online accounts

Make it Strong and Smart



Best Practices to keep your password Safe & Secure

Personal Information in password makes it a weak password

Regularly change and avoid repeating the password

Keep your passwords as secret even from your family members

p@$$w0rd

****

Create personalized pass phrases as Password following password creation criteria

Supported by

certin
Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

myGov
मेरी सरकार

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

सी-डैक
CDAC