APAC Cybersecurity Fund

The Asia Foundation

Module 4

Passwords, Password Management, and Two-Factor Authentication

implemented in India by

with support from Google.org

Training Module developed under the project **APAC Cybersecurity Fund**

This training module is designed to provide general information and guidance on cybersecurity best practices. While every effort has been made to ensure the accuracy and relevance of the content, the information provided is for educational purposes only and does not constitute professional advice or an exhaustive cybersecurity strategy. By participating in this training, you acknowledge and accept that the information is provided "as is," without any guarantees or warranties of any kind, express or implied. For tailored cybersecurity solutions, please consult with certified experts.

Organized by **The Asia Foundation**

Implemented in India by **The Foundation for MSME Clusters**

Supported by **Google.org**

Module also available in Hindi, Marathi, Punjabi, Kannada and Telugu

Module developed by **Global Cyber Alliance** & **CyberPeace Foundation**

Module designed by **Chowdhury, Basu & Ray**

Version 1.0 December, 2024

Module 4

What We Will Talk About

Passwords, Password Management, and Two-Factor Authentication

One of the most common ways hackers gain access to your accounts, network, and information is to log in as you.

Hacking passwords is easier than ever. Programs are available that can crack a password in seconds or minutes.

People often reuse the same password, which means once an unauthorized user has gained access to one of your accounts, they've effectively gained access to them all. It is important that you use a unique password for every account to prevent this from happening to you.

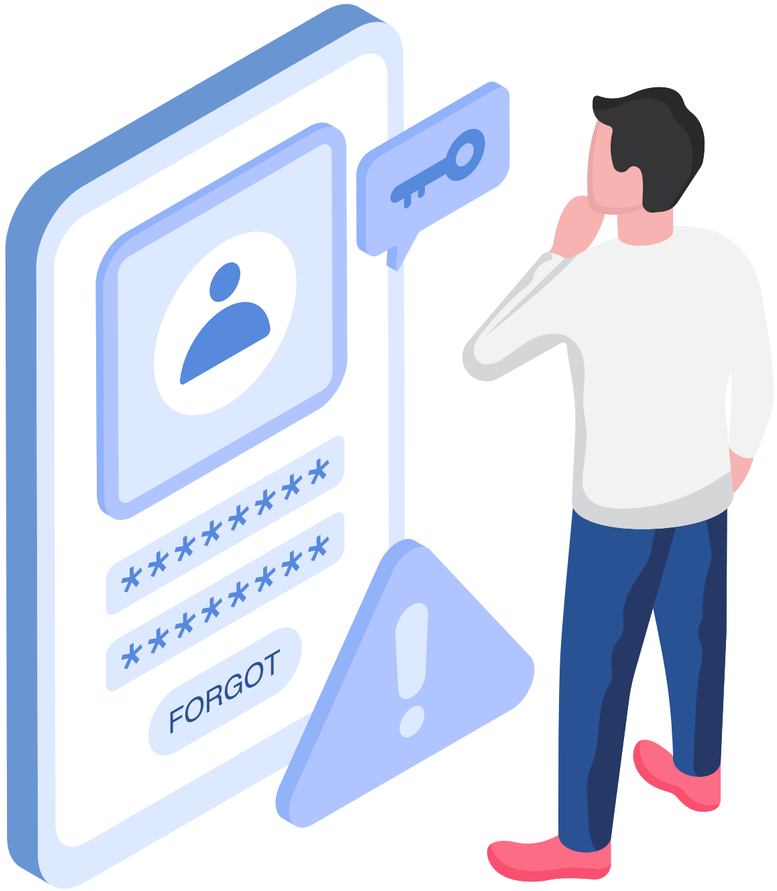
1. WHY STRONG PASSWORDS MATTER
2. HOW CRIMINALS GAIN ACCESS TO YOUR PASSWORDS
3. CREATING STRONG PASSWORDS AND PASSPHRASES
4. STRONG PASSWORD CHECKLIST

Strong passwords helps to:

- Protecting your identity
- Financial security
- Protecting your business reputation
- Preventing unauthorised access to your business' social media accounts
- Protecting operations
- Preventing supply chain disruptions

How Criminals Gain Access to Your Passwords:

Once criminals get a password, they can easily sell it on the ‘dark web,’ which is an illicit market on the Internet for buying and selling sensitive data. There are many techniques criminals use to access passwords:



Passwords, Password Management, and Two-Factor Authentication

Password Hacking Methods

Passwords, Password Management, and Two-Factor Authentication

There are many techniques criminals use to access passwords:

- **Social engineering:** Criminals are very skilled at manipulating conversations and using various unexpected ways (a phone call, text message, or social media) to appear legitimate and trick you into revealing your passwords and other personal information. Phishing emails are the most common type of social engineering attack.

- **Manual guessing:** Using personal information like names of sport teams, pet names, or date of birth to guess part of your password. They often get this information from public sources or even from your own social media posts. During the pandemic, attackers exploited default or predictable passwords like "password123" or "admin" on healthcare MSME systems, gaining unauthorized access to sensitive patient data.

- **Credential stuffing:** Once one account has been compromised, they will try the same username/password elsewhere. The Zomato breach (2017) exposed 17 million user records. Stolen credentials were reused in credential stuffing attacks on other platforms where users reused passwords.

- **Credential stuffing:** Once one account has been compromised, they will try the same username/password elsewhere. The Zomato breach (2017) exposed 17 million user records. Stolen credentials were reused in credential stuffing attacks on other platforms where users reused passwords.

Passwords, Password Management, and Two-Factor Authentication

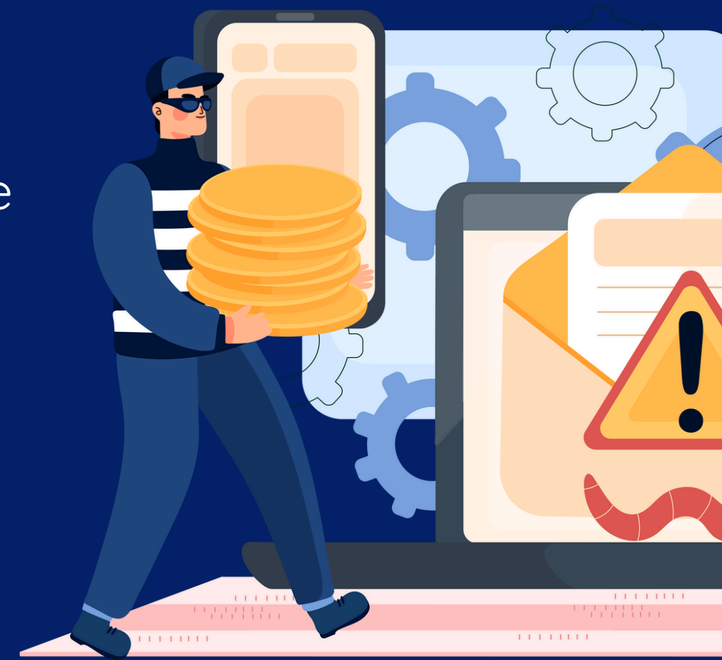
- **Dictionary attack:** A form of brute force attack that uses known dictionary words/phrases or common passwords.
- **Shoulder surfing:** In a public place, or even at your desk, there may be someone watching your activity.
- **OTP Related Scams:** Fake “bank official” calls ask citizens to share OTPs to "validate" accounts, leading to large-scale fraud in UPI transactions. These scams constituted a significant portion of digital payment fraud in 2023.
- **Credential stuffing:** Once one account has been compromised, they will try the same username/password elsewhere. The Zomato breach (2017) exposed 17 million user records. Stolen credentials were reused in credential stuffing attacks on other platforms where users reused passwords.
- **Ransomware/ Malware:** This refers to malicious software that encrypts data (ransomware) or damages systems (malware), demanding a ransom for recovery or exploiting vulnerabilities to steal sensitive information. The WannaCry ransomware attack in 2017 affected Indian MSMEs reliant on outdated Windows systems, causing massive data loss and operational shutdowns.

Passwords, Password Management, and Two-Factor Authentication

- **Keylogging Tools:** Software or hardware tools that record every keystroke made on a device, capturing sensitive information like passwords, account details, and personal data.

- **Credential Theft & Reuse:** Cyber criminals will steal passwords or credentials and then use them across multiple platforms where the victims are likely to have reused the same login credentials. One account breach sets off a chain of breaches. Leaked Aadhaar credentials were reused in multiple fraudulent financial activities, showcasing the dangers of credential reuse across platforms

- **Unsecured Networks & Public Wi-Fi:** Open, unencrypted networks can be targeted to intercept sensitive data and steal potential information. This is especially likely during high-volume traffic/ transactions such as when people use free public Wi-Fi at trade fairs.

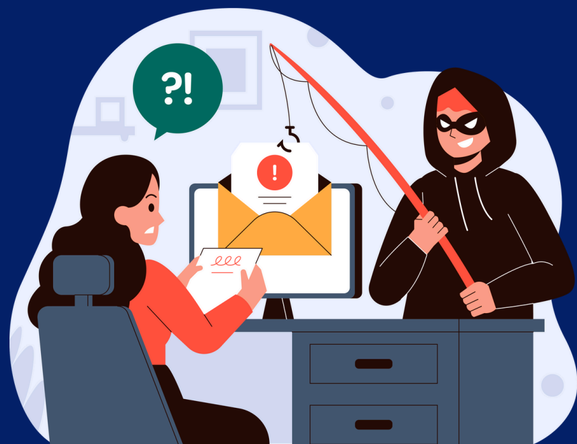


- **Exploiting Unpatched Software:** Cyber criminals will often take advantage of known vulnerabilities in outdated or unpatched software to gain unauthorized access to systems or data.

- **Physical Access:** Direct physical access to or possession of devices can allow malicious actors to bypass remote/ digital security protocols.

- **Account Recovery Exploits and Impersonation Scams:** These refer to fraud schemes where attackers use publicly-available or stolen information to exploit account recovery processes and impersonate legitimate users, thereby seeking “help” to “regain lost access” to other people’s accounts.

- **Leveraging Online Marketplaces:** Cybercriminals posing as sellers or customer service representatives on e-commerce platforms can steal login credentials, payment details, or personal information.



Creating Strong Passwords and Passphrases

Once criminals get a password, they can easily sell it on the ‘dark web,’ which is an illicit market on the Internet for buying and selling sensitive data. There are many techniques criminals use to access passwords:

- Use unique passwords or passphrases for each account
- Keep your passwords or passphrases in a safe place (see later lesson on password managers)
- Do NOT use common words such as “password” or “123456” that are easily guessable
- Do NOT use personal information such as your birthday or your pet’s name
- Do NOT share your password unless it is absolutely necessary (see later lesson for examples of when and the best method to minimize the risk)

Creating Passphrases:

A good way to make your password difficult to crack is by combining three random words. This is called a passphrase and will be easier for you to remember than a password with many different characters, numbers, and upper/lowercase letters. It will also be more unpredictable and harder for a criminal to guess or crack.

Tips for creating passphrases:

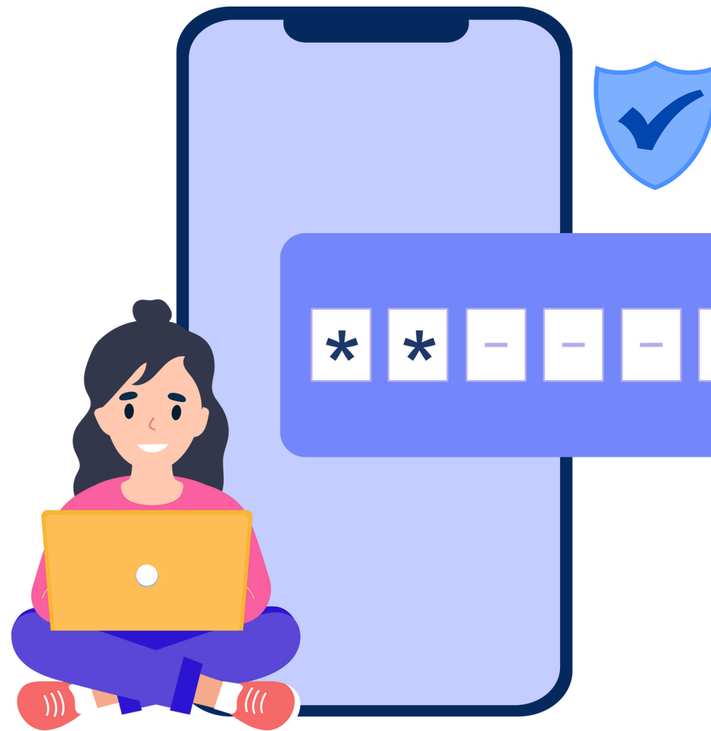
- Choose relatable words
- Avoid predictable famous phrases like “unity in diversity”
- Use your regional identity
- Use your personal interests
- Go for phrases and words that are meaningful to you but hard to guess for others
- Ensure a minimum of three to four words

Creating complex passwords:

A password made up of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password containing only lowercase letters.

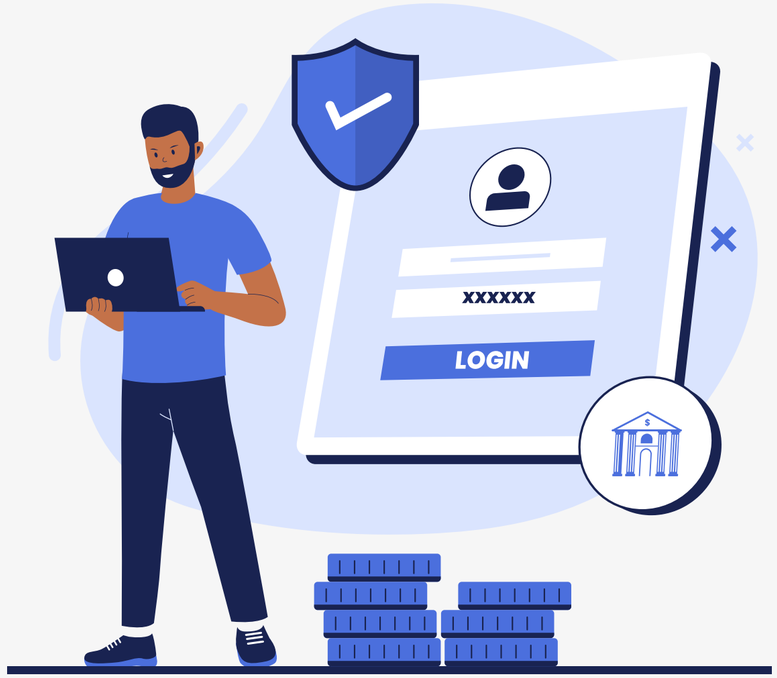
Here are some tips:

- Use a password manager to create and store them for you (see later lesson on password managers)
- Or you can create your own. A good system to use is taking a 3-4 word phrase and combining symbols, numbers, and letters to spell out.
- Example: I love birthday cake = il0v3b1rthd@yc@k3!
- Here are some great examples for the Indian audience: Ganga#Diwali@Namaste or Kerala_Coconut#123 or SpicySamosa@56%



Sharing Account Login:

Sharing of account login information is understandably a very convenient way to save costs as an MSME, however, it brings greater risk to your business. Sharing account login information is never recommended, however, some online platforms commonly used by small enterprises only allow one user login. And that is just not very practical. So let’s talk about safer ways to share that login information.



Top tips:

- Never share the username and password or passphrase in one message such as a single email or single text. If this is intercepted, then someone else will have full access to that account.

- Never share the information if asked by someone else if it is not a conversation you have initiated, especially if you get a request from a phone number you do not recognize, or an email asking you to click on a link to share it.

- Speak directly to the person you need to share the information with, preferably by video call or a mobile call that you have initiated to a known number. Use this opportunity to share the information in real-time over video or call so there is no record of it.

- If you must share it via email, test, or messaging app, split the information using different methods and delete those messages after wherever possible.

  Example: Username by email and password or passphrase by text or messaging app.

- If you are using two-factor or multi-factor authentication (2FA/MFA) for that account (Congratulations!) then use a third method to give the 2FA code. If you are not using 2FA/MFA yet, please check the later lesson to learn more! Most MSMEs in India will use Gmail for operations. If you're already using 2FA.

Here are some additional layers of security you can introduce into your operations:

- Use an authenticator app like Google Authenticator for generating 2FA codes without requiring SMS.
- Use an alternative email ID registered specifically for recovery, ensuring access even if the primary phone is unavailable.
- Use Indian-specific SMS-enabled banking apps or UPI apps to familiarize employees with secure authentication systems, as they often overlap with personal 2FA experiences.
- If Remind your employees and team members that banks like SBI and ICICI use OTP-based MFA as a standard for their net banking services. This establishes the importance of using multilayered security protocols for all important transactions and processes.

Using a Password Manager

Do you have several or more accounts to manage? Feeling unsure of how you are going to create, save, and remember all of those unique passwords or passphrases we've been discussing? The use of a password manager tool is a great way to navigate all of these challenges. Password managers create and store unique and complex passwords for each of your accounts. Setting up your password manager account will take a small investment of time, but it is well worth it and easy to maintain and update after that initial setup. You will then only need to remember one password (using the skills you already learned on how to create a strong password or passphrase) for the password manager tool itself.

Helpful things to know about password managers:

- You can integrate biometric authentication for an extra layer of security, especially useful for mobile devices in BYOD settings.
- Password managers can help enhance security and manage access for distributed teams with remote workers.
- Strict onboarding and off-boarding protocols must be followed for organisational passwords. Ensure all passwords are changed or removed when employees join or leave.
- While there are several globally-popular tools that can help you with password management, there are some great indigenous options too. Use local solutions (e.g., K7 Password Manager) along with global tools like LastPass or Dashlane.
- MSMEs can prioritise low-cost, India-made solutions when upgrading their security features. The DigiLocker is a key example of Indian security and data management options.Bitwarden is a free, open-source password manager that is secure, ZoHo Password Vault is also recommended.:

Following Safe Password Practices For Online Browsing

Most major Internet browsers also allow you to save your passwords, which is very convenient (and free), however, there are some important things to remember when using them.

Passwords, Password Management, and Two-Factor Authentication

Top tips:

- If you share your device (mobile, tablet, laptop, or desktop) with employees or family members, you are essentially giving them the same access that you have to all of those accounts. This is extremely risky. Don’t save passwords on shared/ public devices

- Ensuring you have two-factor or multi-factor authentication (2FA/MFA) in place for all accounts that allow it is a great layer of additional security to reduce this risk, especially if you choose to require 2FA/MFA for each login. This way, a family member cannot inadvertently access an account without your permission.

- Consider the level of sensitivity of the account you are accessing using this method - is it your banking account? Payroll? Customer data? The more sensitive the data, the more you should be wary of using browser-based password management. A separate tool may be more appropriate for your business.

Passwords, Password Management, and Two-Factor Authentication

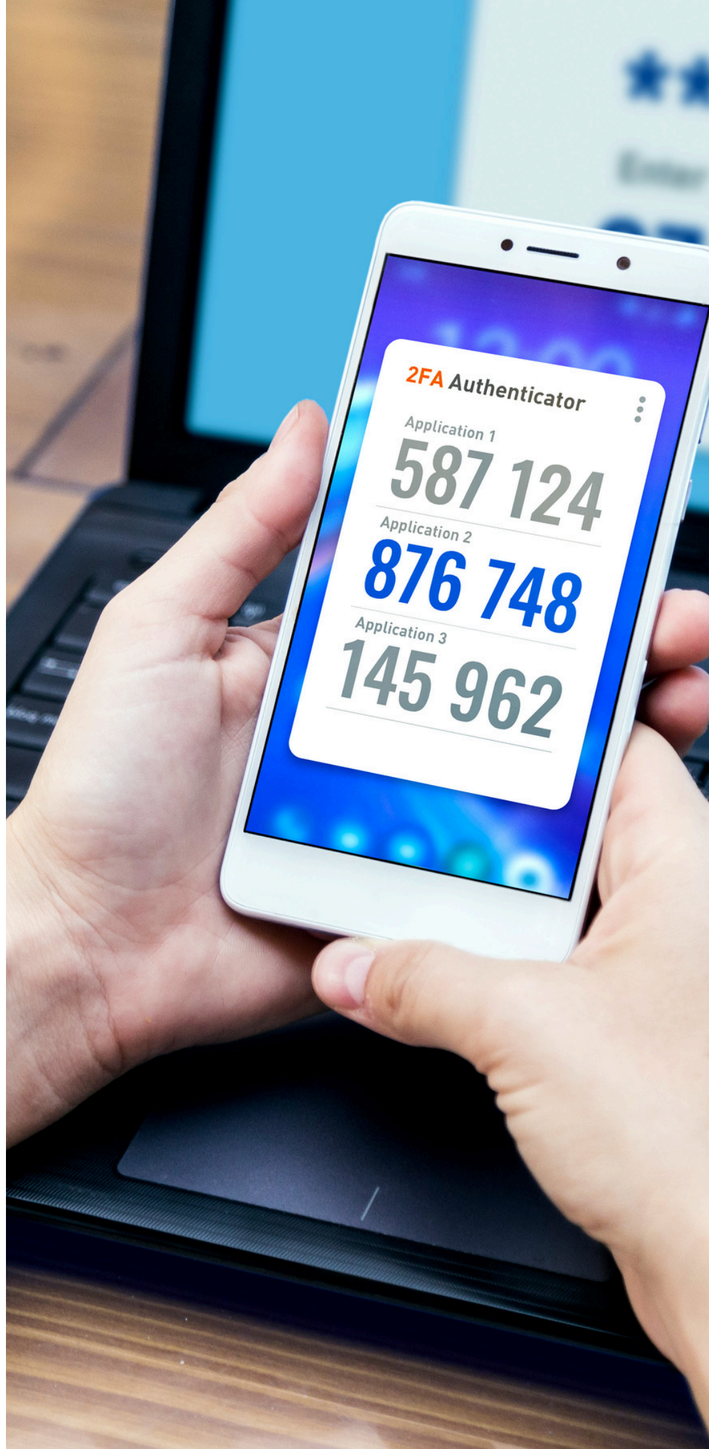
Two-Factor or Multi-Factor Authentication

- Two-factor authentication (2FA), also known as multi-factor authentication (MFA), must be used whenever possible. 2FA requires two separate pieces of information before it gives you access to your account.

  1. Your password or passphrase
  2. Something unique to you. Examples:

- A code that times out using a third-party tool such as Google Authenticator or Microsoft Authenticator
- A code that is sent to your phone or your email
- A biometric, such as a fingerprint or your face

Some accounts only allow one user/admin for the account, so only the main admin can “own” the 2FA code. This creates an extra step in the login process when others have to share those login credentials, however, consider it an additional layer of protection in the event someone gains access to your password or passphrase. Without this code, that person will not be able to gain access to your account. Remember the tips in the lesson talking about sharing login information to accounts and treat it using those same tips.



Passwords, Password Management, and Two-Factor Authentication

A lot of MSMEs in India use Amazon for their e-commerce activities. Since Amazon permits only one admin to set up 2FA, the business owner typically uses their mobile number for the authentication code. Team members needing access must coordinate with the owner to retrieve the 2FA code during login.Treat the 2FA code like an OTP for UPI payments: critical, sensitive, and only to be shared with verified individuals when absolutely necessary.

- Here's a quick list of things to keep in mind regarding 2FA and MFA:

- Enable 2FA for critical accounts (e.g., banking, emails).

- OTPs via SMS or app-based 2FA add a layer of protection.

- Consider MFA options (e.g., biometrics) for added security.

- Be mindful of attempts to extract OTPs and authentication codes - scammers will often call and post as legitimate authorities or service providers and ask for these codes. They might refer to them by other names to confuse you into sharing said digits.

- For accounts that give you a list of recovery codes upfront - store the same in a secure place, ideally not on the device in question.

Strong Passwords Checklist

- **Password Length:** Minimum of 8-12 characters or more.
- **Password Complexity:** Require a combination of uppercase, lowercase, numbers, and special characters.
- **Password Uniqueness:** Enforce unique passwords for each account or system or device. No password reuse.
- **Password Expiration:** Require regular password changes, e.g., every 60-90 days. Prevent reuse of previous passwords.
- **Password Storage:** Store passwords using secure hashing algorithms, never in plain text.
- **Password Management**: Encourage password managers and prohibit password sharing or writing them down insecurely.
- **Password Reset:** Implement secure procedures with multi-factor authentication for password resets.
- **Password Auditing**: Regularly audit password strength and compliance and monitor for compromises.
- **Password Protection:** Use key-based authentication along with passwords where possible.
- **User Awareness:** Provide training on password best practices and risks of weak passwords.
- **Policy Enforcement:** Define mechanisms for enforcing the policy and procedures for granting exceptions.
- **Policy Review:** Regularly review and update the policy to align with best practices and emerging threats
- **Complex Words:** Avoid using passwords that consist of simple dictionary words.
- **Personal Information:** Avoid passwords such as your birthday or your pet's name.
- **Simplistic Passwords:** Don't use common words like "password" or "12345" as these are easily guessed
- **Passphrases:** Use a series of unrelated words (e.g., "sunflower_eagle!forest") for added complexity without compromising memorability.
- **Password Sharing:** Do not share your password unless absolutely necessary.
- **Monitor for Breaches:** Periodically check if your email or password appears in data breaches via services like Have I Been Pwned.

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 5

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at helpline@cyberpeace.net or on WhatsApp at +91 957-00-000-66

Training Module developed under the project **APAC Cybersecurity Fund**

implemented in India by Foundation for MSME Clusters (FMC)

with support from Google.org