# HOW TO PROTECT YOURSELF FROM SOCIAL ENGINEERING

## Use long passphrases

Passphrases are longer and more complex than typical passwords, making them much harder to crack. Choose a random sequence of words (e.g., "PurpleMonkeyDeskLamp") that doesn't follow any predictable pattern.

## Avoid common passwords

Simple and frequently used passwords (e.g., "123456," "Password1!") are easy targets for AI. Avoid using anything easily guessable, like personal information or words found in a dictionary.

## Enable multi-factor authentication

MFA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone. Even if your password is compromised, MFA can prevent attackers from accessing your accounts.

## Use a password manager

Password managers can generate and store complex, unique passwords for each account. This eliminates the need to remember multiple passwords while ensuring that all your accounts have strong protection.

## Update passwords when needed

If you suspect you are part of a breach or if your credentials have been compromised in a data leak, change your password as soon as possible. Updating passwords reduces the chance that older credentials can be used against you.

## Monitor for data breaches

Use services that notify you when your email or password is part of a data breach. By staying alert to leaked credentials, you can take immediate action to secure your accounts.

## REMEMBER

**AI makes password attacks faster and more efficient. With strong passwords, passphrases, and multi-factor authentication, you can protect yourself from these advanced attacks.**

## QUICK TIPS

**Use passphrases**—long, random combinations of words are much harder for AI to crack.

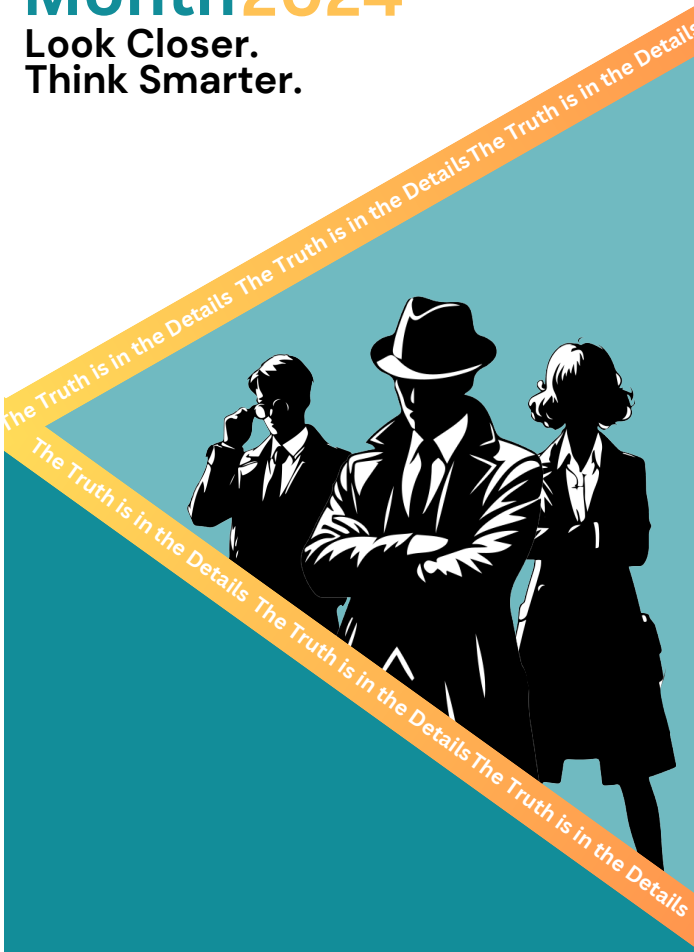
**Avoid personal information**—don't use names, birthdays, or any easily found data.

**Enable MFA**—add a second layer of security beyond just your password.

**Use a password manager**—generate and store strong passwords for every account.

# Cyber Security Awareness Month 2024

**Look Closer.**
**Think Smarter.**




# Protect Your Passwords from AI-Powered Attacks

# WHAT ARE PASSWORD ATTACKS?

AI-powered password attacks use advanced algorithms and machine learning to guess or "crack" passwords at an incredibly fast rate.

There are several types of password attacks that allow attackers to login. When these attacks are performed by AI, it enables the attacker to draw on large datasets including information found online, stolen passwords and use these to guess passwords.

## Common types of password attacks

### Brute Force Attack

Attackers use programs to try every possible combination of characters, numbers, and symbols until the correct password is found. AI enhances this by speeding up the process and detecting patterns that reduce the time needed.

### Dictionary Attack

In this method, attackers use AI to test words or phrases from precompiled lists of commonly used passwords or phrases. AI can analyse these lists and improve its ability to guess more complex or customised variations.

### Credential Stuffing

Attackers use previously leaked username and password combinations across multiple platforms. AI helps automate this process, rapidly testing stolen credentials on various sites.

### Rainbow Table Attack

A Rainbow Table Attack uses large pre-generated databases of common passwords to quickly match them with stored passwords. Attackers use this method to break into accounts with weak or common passwords.

### Password Spraying

Attackers use AI to test commonly used passwords (like "Qwerty! or "Password1!") across many accounts, avoiding detection by targeting only a few passwords per account to prevent locking users out.

## RED FLAGS OF WEAK PASSWORDS

- Using personal information, such as names or birthdates, especially if found on social media.
- Short passwords under 12 characters.
- Common phrases or dictionary words like "welcome123" or "Qwerty12345!"
- Reusing passwords across multiple accounts.