How to safeguard against 5 key threats to password security

Every year, on the first Thursday of May, World Password Day is celebrated to raise awareness about the importance of password security, password-related cybersecurity threats, and the best practices users and organisations can employ to safeguard their passwords, and thus their systems.

Let us examine some of the most significant threats to password security:

Phishing

Phishing involves a hacker contacting a victim while posing as a legitimate representative of a trusted entity (such as a bank, government agency, educational institute etc.) to trick them into revealing their passwords and other sensitive information.

While many users are alert and aware of the dangers of phishing scams, they continue to evolve in their sophistication: from spear phishing (hackers targeting specific individuals while impersonating a close contact) to URL hijacking (creating false websites with nearly-identical domain names to trick visitors into entering their credentials) and more.

Brute force attacks

Brute force attacks involve hackers systematically trying out different password combinations until they can successfully gain access to an account or system.

Simple passwords (such as '123456', birthdays or other personal details about the user etc.) are particularly vulnerable to such attacks.

The methodology has evolved with Hybrid brute force attacks leveraging automated tools (including AI-powered tools) that can try thousands of password permutations in seconds.

Credential stuffing is a related form of cyber-attack wherein hackers use passwords stolen in one successful data breach to attempt to access different accounts of the same users. Reusing the same passwords (or variations) across multiple accounts makes users highly vulnerable to this.

Man-in-the-Middle attacks

Man-in-the-Middle attacks are caused by poorly secured communication channels, wherein cyber-attackers intercept authentication messages between servers and clients.

The hacker monitors users logging into an insecure website. This login data is relayed to the hacker, who then redirects the user to a false website. Users navigate through this false website, believing they are securely accessing their data, while unwittingly feeding malicious actors their passwords and other sensitive details.

Keylogging

A more sophisticated method of password theft, keylogging involves hackers installing surveillance software onto user's devices (through malware, or through a USB drive or keyboard attachment directly connected to the device) to record every keystroke the user makes. This enables the hacker to derive the users' passwords and other confidential information.

Password spraying

Account lockouts are an important tool in the fight to ensure password security. Password spraying has emerged as a method developed by hackers to counteract this safeguard.

Most account lockouts are triggered by making too many login attempts during a short time. Hackers exploit this by trying the same password across multiple websites, before trying the next possible password. By the time the hacker has exhausted all the websites on their list and circled back to the first website with a new password, the lockout policy has reset and the previous failed attempt is not counted. In this manner, hackers can make a much greater number of attempts to crack passwords and gain access to accounts.

How to enhance password security?

Human users are unfortunately a significant weak link in the chain of password security. At an organisational level, there is a need to rigorously enforce policies around password generation, management and use. Users should use short and simple word and character combinations, or personal details, as passwords. More complex passwords, including auto-generated passwords, will provide a much stronger defence against brute force attacks.

Users should also maintain constant vigilance about possible phishing scams and verify the legitimacy of any individual with whom they communicate and/or any website or app that they visit, before sharing or entering any confidential information.

Multi-factor authentication (MFA) provides an additional layer of security to accounts, frustrating hackers' attempts to gain unauthorised access even if passwords are compromised. The use of password managers, to generate and securely store complex passwords in an organised and encrypted manner, further elevates password security in addition to offering users a more frictionless experience.

The ramifications of poor password security can be severe for individuals and organisations – from account takeovers by malicious actors, to the compromise of sensitive data. Thus, it is critical to take effective measures to enhance password security.