Strong Passwords and Multi-Factor Authentication

A password is the lock on most of our accounts, and attackers try to open it in many ways. They guess common passwords, try passwords leaked from other websites and trick people into revealing them. The guidance of the US National Institute of Standards and Technology, known as NIST, shapes much of today's advice. It favours length over complicated rules, and it supports password managers and extra verification steps. Tamer, an office manager, improves the security of his accounts with four habits.

1. Long Passphrases

The first habit is to prefer long passwords. A passphrase made of several random words is easier to remember than a short and complicated password, and it is much harder to guess. NIST advises against forcing special characters and regular changes, because people then choose predictable patterns. Words that are linked to our name, birthday or favourite team are weak, even when they are long. Length and unpredictability together create strength.

Example: A family replaces the Wi-Fi password with four unrelated words that they can remember. Using a long passphrase, they get a password that is easy for the family to remember and hard for a stranger to guess.

At work: Tamer changes his email password from a short code with symbols to four unrelated words. Using a long passphrase, he remembers it without notes, and guessing programs would need far longer to crack it.

2. Unique Passwords and a Manager

The second habit is to use a different password for every account. When a website leaks passwords, attackers try the same combination on other sites, so one reused password can open many doors. Nobody can remember dozens of long passwords, so a password manager stores them safely and fills them in. Only one strong passphrase is needed to unlock the manager. NIST guidance supports the use of password managers.

Example: Imagine that a shop leaks its customers' passwords. Because we used unique passwords stored in a password manager, our bank account stays safe, as its password was different.

At work: Tamer finds that he used one password for six work tools. With unique passwords and a password manager, he creates a new one for each tool, so a leak at one website no longer threatens the others.

This document is a property of Asaseeyat Academy - © Copy Right Protected.

3. Add a Second Factor

The third habit is multi-factor authentication, also called MFA. It asks for two or more different kinds of proof: something we know, such as a password, something we have, such as a phone or a security key, and something we are, such as a fingerprint. Even if an attacker steals the password, the second proof is still missing. Email, banking and work accounts are the best places to start. Setting it up usually takes only a few minutes.

Example: A bank asks for a password and then for a code from an app on our phone. Using a second factor, a thief who knows the password still cannot enter the account.

At work: Tamer turns on MFA for the company email. Using a second factor, he blocks a login attempt from another country, because the attacker has the password but not his phone.

4. Choose Stronger Methods

The fourth habit is choosing the strongest second factor available. Codes from an authenticator app or a physical security key are generally safer than codes sent by text message, because text messages can be intercepted or redirected. Security keys and passkeys can also resist fake websites, since they check the real address. We never share a code with anyone, and we change a password when there is a sign that it was exposed. Backup options should be saved safely in case a phone is lost.

Example: A family member's phone number is taken over by a scammer, so text codes reach the wrong person. Choosing a stronger method, the family member moves to an authenticator app, and codes stay on the phone.

At work: Tamer gives the finance team security keys for the bank portal. Choosing a stronger method, he makes it much harder for a fake login page to steal access.

Conclusion

In summary, strong account security rests on four habits. We use long passphrases, a different password for each account, a second factor and the strongest second factor available. NIST guidance supports length, password managers and extra verification, and it advises against forced complexity and routine changes. Tamer's accounts are now much harder to break into. Small changes made once give protection every day.

Sources

- NIST Special Publication 800-63B: Digital Identity Guidelines, Authentication and Authenticator Management – https://pages.nist.gov/800-63-4/sp800-63b.html
- CISA (US Cybersecurity and Infrastructure Security Agency): Use Strong Passwords – https://www.cisa.gov/secure-our-world/use-strong-passwords
- UK National Cyber Security Centre (NCSC): Three random words – https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

This document is a property of Asaseeyat Academy - © Copy Right Protected.