T2025_20 Avoid Reusing Passwords Across Accounts (September 27, 2025)

Reusing the same password across multiple accounts increases your risk of a **domino-effect breach**. If one site is compromised, attackers can use that same password to access your email, bank accounts, cloud storage, or workplace systems. This is a tactic known as **credential stuffing**. Even a strong password becomes useless once exposed in a data breach, as attackers use automated tools to test leaked credentials across multiple platforms within seconds.

Always use unique passwords for each account, especially for sensitive services like email, financial portals, or work systems. To manage them securely, use a **trusted password manager** to generate and store strong, random passwords.

References

- OWASP Foundation. (n.d.). Credential stuffing. OWASP. Retrieved September 26, 2025, from https://owasp.org/www-community/attacks/Credential_stuffing

- Cloudflare. (n.d.). *Credential stuffing: What it is and how to prevent it*. Cloudflare. Retrieved September 26, 2025, from https://www.cloudflare.com/en-gb/the-net/credential-stuffing/