Cyber Secure

Module 3

Password Management

Author: George Nicholl

Student ID: 50095130

Passwords are the first line of defence in securing digital accounts, yet weak password practices remain one of the most common and dangerous cybersecurity vulnerabilities. This module explores essential password management techniques, the impact of poor password hygiene and tools like password managers and multi-factor authentication (MFA) that can dramatically reduce risk.

This content expands on the associated training video and provides additional technical and practical guidance for individuals and organisations.

What is Password Management?

Password management refers to the strategies and tools that are used to create, store update and protect digital credentials. Poor password hygiene – including reusing passwords, using predictable formats or ignoring MFA, all open the door to credential stuffing, data breaches and account takeover attacks.

According to Verizon's 2023 Data Breach Investigation Report, 81% of hacking-related breaches were caused by stolen or weak passwords. A 2024 NordPass survey also revealed that 64% of users reuse passwords across multiple accounts, greatly increasing their vulnerability.

Common Threats or Mistakes

A. Using Weak or Predictable Passwords

- Common choices such as "123456" or "password" are still widely used
- Easily cracked through brute force or dictionary attacks

B. Reusing Passwords Across Accounts

- One breach can compromise all linked services
- Facilitates credential stuffing attacks

C. Sharing or Storing Passwords Insecurely

- Writing passwords down or sharing via email or messages
- Passwords may be accessed b unauthorised users

D. Ignoring Multi-Factor Authentication (MFA)

- Lack of MFA leaves accounts vulnerable even if credentials are stolen
- MFA can block 99.9% of account takeover attempts (Microsoft, 2023)

Real World Examples

- **2019 Facebook Password Leak** – Over 600 million passwords stored in plaintext were exposed internally
- **Colonial Pipeline (2021)** – Reused credentials were linked to the attack that shut down major infrastructure.
- **Credential Stuffing Attacks (Ongoing)** – Automated use of leaked username/passwords remains a leading threat to personal and corporate accounts.

Reducing Password Compromises

A. Create Strong Passwords

- Use at least 12-16 characters
- Mix uppercase/lowercase letters, number and special characters
- Avoid using names, birthdays or dictionary words

B. Use a Password Manager

- Securely stores and encrypts all passwords
- Generates strong, unique credentials for each site
- Auto-fills login forms only on verified pages

C. Enable Multi-Factor Authentication

- Combines something you know (password) with something you have (app/device) or are (biometrics)
- Reduces risk of credential compromise

D. Monitor for Data Breaches

- Use tools like “Have I been Pwned” to detect if your credentials have been leaked
- Update passwords immediately if exposed

Key Takeaway

Effective password management is essential for modern cybersecurity. Weak or reused passwords remain as one of the most preventable yet exploited entry points for attackers. By adopting strong password creation habits, enabling MFA and using password managers, individuals and organisations can significantly lower their risk of a breach. Cyber hygiene starts with good password practices - taking simple steps today can prevent major security incidents tomorrow.

Why This Matters for You

Cybersecurity starts with individual responsibility. While organisations invest in technology, it only takes one weak password to bring down entire systems. Good password practices protect your identity, your data and your organisation.

Quick Recap: Password Management Best Practices

DO:

- ✔ Use a password manager to store and generate strong credentials
- ✔ Make passwords at least 12 characters long and include a mix of uppercase/lowercase, numbers and symbols
- ✔ Enable multi-factor authentication (MFA) wherever possible
- ✔ Change passwords regularly, especially after a known breach

DON'T:

- X Don't reuse the same password across multiple services
- X Don't store passwords in browsers or unsecured documents
- X Don't ignore MFA prompts or turn them off for convenience

References

CISA (2024) *The Importance of Password Managers*. Cybersecurity & Infrastructure Security Agency. Available at: https://www.cisa.gov

Dashlane (2024) *Time Saved Using Password Managers*. Available at: https://www.dashlane.com

Google (2023) *The Impact of MFA on Phishing Attacks*. Available at: https://security.googleblog.com

Hive Systems (2024) *Password Cracking Times*. Available at: https://www.hivesystems.io

Hunt, T. (2024) *Have I Been Pwned: Data Breach Statistics*. Available at: https://haveibeenpwned.com

LastPass (2023) *Password Sharing Habits in the Workplace*. Available at: https://www.lastpass.com

Microsoft (2023) *Why Multi-Factor Authentication Matters*. Available at: https://www.microsoft.com/security

NordPass (2024) *The Most Commonly Used Passwords*. Available at: https://nordpass.com/most-common-passwords

Specops Software (2024) *How Often Do People Change Their Passwords?*. Available at: https://www.specopssoft.com

Verizon (2023) *Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/dbir/