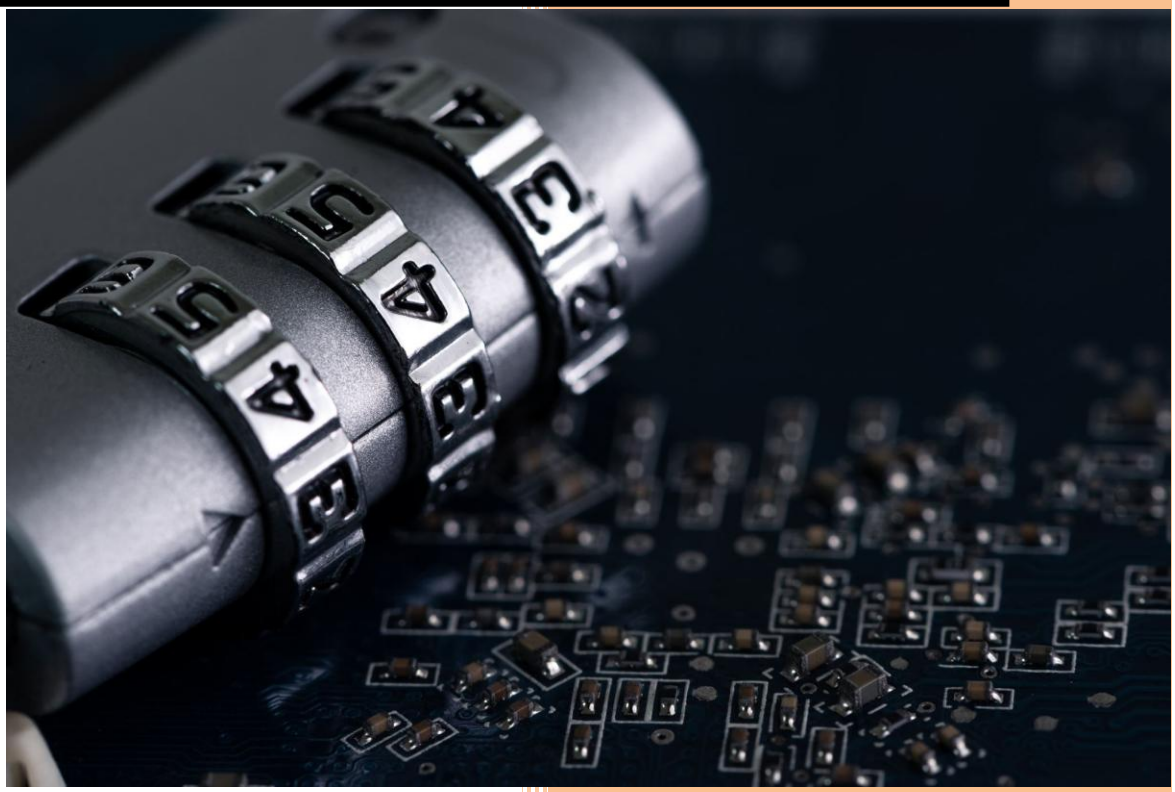
Estimated Reading Time: 4 Minutes

Passwords

Security Awareness Training



William Fisher

3/18/2025

Passwords

Why Do We Have Passwords?

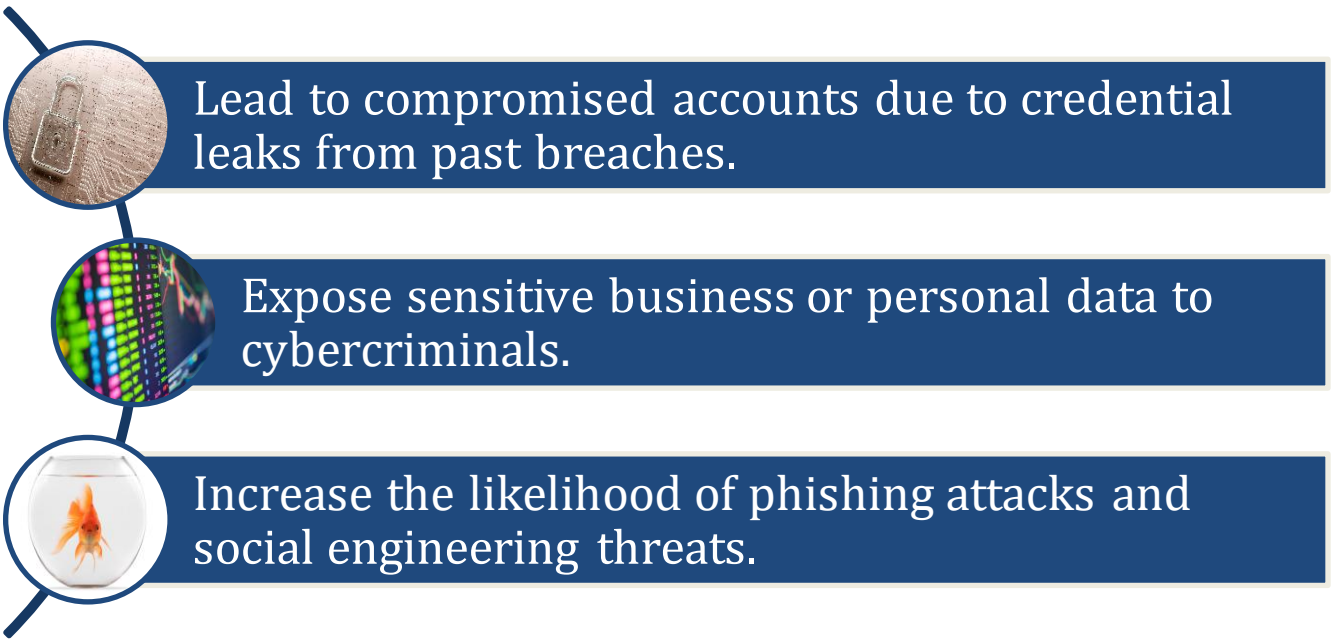
Passwords act as the first line of defense against unauthorized access to personal and organizational accounts. They help ensure that only the rightful owner can access sensitive information, protecting against data breaches, identity theft, and cyber threats.

Why Shouldn't We Share Passwords?

Sharing passwords compromises security by increasing the chances of unauthorized access and reducing accountability. If multiple people have access to the same credentials, it becomes difficult to determine who performed specific actions, leading to security gaps. Even if shared with a trusted colleague or friend, that person might store or share it insecurely. Additionally, passwords can be accidentally exposed, such as by leaving a note on a desk or falling victim to a phishing attempt. Once a password is known by others, it can be misused, leading to data leaks, account takeovers, and security breaches.

Why Ignoring Security Policies is Dangerous.

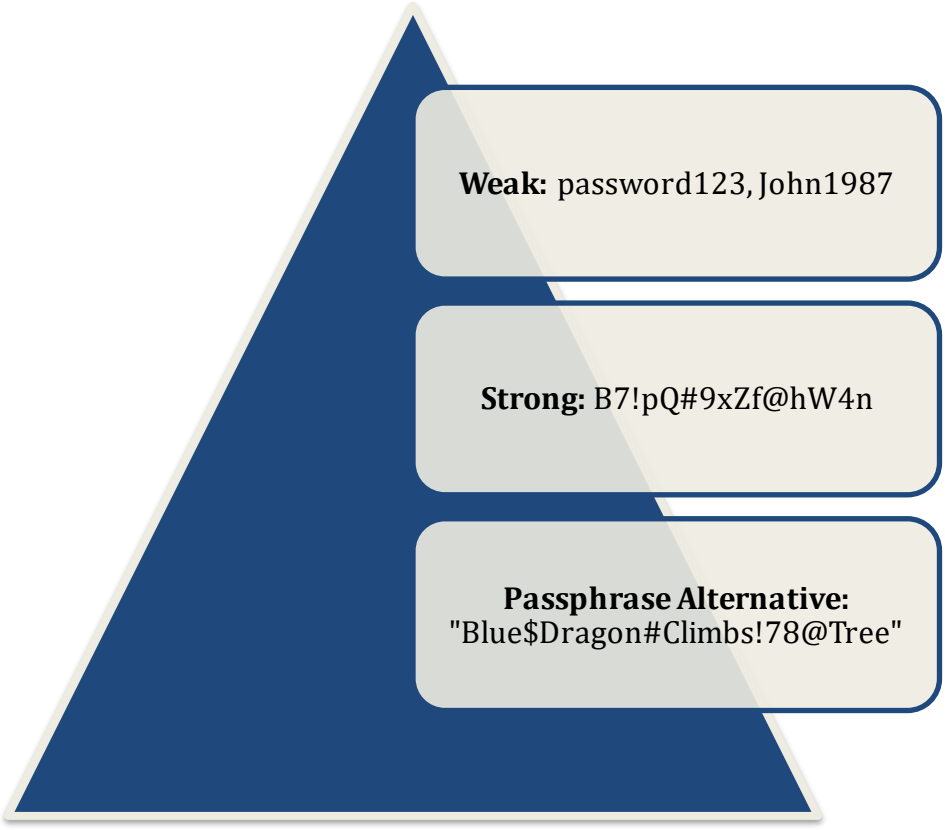
Organizations and websites enforce password policies to mitigate risks. Circumventing these policies by using weak passwords, using sequential passwords (e.g., password1, password2), or reusing passwords across accounts can:



What Does a Strong Password Look Like?

- At least **8 characters** long.
- A mix of **uppercase and lowercase letters, numbers, and special characters**.
- **Unique** for each account (never reused across different sites).
- **Unpredictable** (avoid common words, phrases, or personal details like birthdays or pet names).

Examples of Strong vs. Weak Passwords:



Best Practices for Storing and Remembering Passwords.

Use a Password Manager: A reputable password manager (like Bitwarden, 1Password, or LastPass) securely stores and auto-fills passwords.

Create a Passphrase: A long but memorable sentence (e.g., "MyDog@te3bonesToday!") can be secure and easier to remember.

Segmenting Passwords: Dividing a random string of characters with underscores, dashes, or spaces enhances memorability while preserving security (e.g., Ahng-Bna#-&7gl).

Write It Down Securely: If necessary, store passwords in a locked, physical location (never in plain text on a device).

Securely Resetting a Password

When a password is forgotten, keep in mind the following information:

Use the Website's Official Recovery Option: Always avoid third-party tools or emails asking for credentials.

Identity Verification: Many services require answering security questions or sending a reset link to a verified email address or phone number to confirm the user's identity before allowing a password reset.

Enable Multi-Factor Authentication (MFA): Once reset, enable MFA for an additional layer of security.

Change Other Accounts If Necessary: If the forgotten password was reused elsewhere, update all related accounts to prevent credential stuffing attacks.

Conclusion

Practicing good password safety protects personal information, organizations, finances, and identities. Following security policies, using strong passwords, and managing them effectively significantly reduces risks such as identity theft and financial fraud. Although password safety can be challenging to implement, the effort provides long-term protection against costly and stressful security breaches. Maintaining vigilance and prioritizing security in digital habits is essential.