

CYBER-SECURITY ESSENTIALS

Password Management Best Practices

Strong passwords are one of the first lines of defence against cyber-attacks. Developing lengthy, complex and hard-to-guess passwords across your workplace accounts can significantly increase the time and computing power required to crack your credentials, making it far more difficult for cyber-criminals to gain unauthorised access to sensitive systems and data.

With this in mind, it's crucial to understand how to create effective passwords and, in turn, better protect your workplace accounts. This article highlights the key pillars of a strong password and offers additional tips to safeguard your credentials at work.

Key Pillars of a Strong Password

When developing passwords for your workplace accounts, remember these guidelines:

- **Make it lengthy.** Every additional character in a password multiplies the number of possible combinations a cyber-criminal must guess to exploit your credentials. A good password length is generally 15 or more characters. Using a combination of uppercase and lowercase letters, numbers, and symbols can also vastly complicate a hacker's ability to steal your password.
- **Never include personal information.** Cyber-criminals may gather public records and social media posts to uncover your personal information and use these details to compromise your credentials. As such, refrain from incorporating family or pet names, your favourite hobbies or sports teams, or special dates (eg birthdays and anniversaries) within your passwords.
- **Avoid predictable patterns.** Common character combinations (eg "welcome123," "p@ssw0rd," "qwerty" or "letmein") are

among hackers' first guesses when attempting to swipe a password. In many situations, these combinations can be uncovered in mere seconds. The most effective passwords usually involve a string of four or more words or unique characters that form a memorable, albeit random, sentence (eg "@pplesRtheB3stFruit!"). Also known as passphrases, these combinations are often the hardest to crack.

- **Don't reuse or repeat.** If you use the same passwords across different workplace (and personal) accounts, you could be increasingly vulnerable to credential stuffing—a tactic in which cyber-criminals use one stolen password to compromise multiple accounts and associated systems. Make sure you vary your passwords between accounts and never reuse previous combinations.

Safeguarding Your Credentials

Keep in mind that your passwords aren't permanent. Your workplace systems and related applications may prompt you to change your passwords at set intervals (eg quarterly or biannually). It's also best to update your passwords if you suspect that your account has been compromised or if you are notified that a service or platform you use has been breached. When creating your passwords, keep these credentials private. Never, under any circumstances, share your passwords with others.

While you may be tempted to use a physical notebook or a plain-text document stored on



Provided by Philip Gibbs Insurance Brokers

This Cyber-security Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact a legal or insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

a personal device to keep track of all your passwords, this is a dangerous practice, as this confidential information could end up in the hands of a malicious party. Rather, it's important to leverage any password tools and further credential safeguards provided by your employer to keep your accounts safe. These resources may include:

- **Password managers**—A password manager stores and organizes your credentials in a digital vault, often secured by a master password and/or biometric identifier (eg a fingerprint or facial scan). When it's time to sign into your account, this tool automatically enters your login information. Using a password manager can help you maintain unique credentials while removing the burden of memorising these complex combinations.
- **Multifactor authentication (MFA)**—Through MFA, you must confirm your identity by providing extra information, such as a phone number, biometric identifier, one-time security code or approval from a third-party authenticator application, in addition to your password when attempting to access sensitive corporate data and infrastructure. Many companies require MFA to access their networks, perform administrative functions within these networks and use enterprise-level cloud applications.

Talk to your employer to review the specific resources available to you. Furthermore, if you run into any problems when signing into workplace accounts or notice signs of suspicious activity (eg unexpected logins or password reset emails), report these issues immediately.

For More Information

Cyber-security can be challenging, but you don't have to navigate this topic alone. Contact your employer for more information on cyber-security best practices.