Put on an Extra Layer of Security with Multi-Factor Authentication

Multi-factor authentication (MFA) is a simple and effective way to protect your online accounts by requiring extra checks to confirm your identity. With MFA, you'll need more than just a password to log in—such as an authentication code sent via text message.

1 Why Multi-Factor Authentication Matters

Using MFA adds another layer of security, making it harder for someone else to access your account, even if they've discovered your password. By combining two or more factors, MFA increases confidence that the person logging in is really you.

2 MFA typically involves:

- **Something you know:** Such as a password or PIN.
- **Something you have:** Such as a physical token or smartphone app.
- **Something you are:** Such as a fingerprint or facial recognition.

3 Benefits of Multi-Factor Authentication

Adding extra layers of authentication increases your cybersecurity, protecting your personal and financial information. It's an easy way to safeguard against unauthorized access, reducing the risk of cyberattacks.

4 How to Enable MFA

Activating MFA is simple and can be done in the security settings of most accounts, including social media, banking, and email services. Once enabled, you'll be prompted for additional steps when logging in.

For more information, visit https://www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication

Case Study: Why MFA Could Have Helped

Vero received an email about an online purchase she didn't make. After checking her accounts, she noticed unauthorized charges. Hackers had used her password, which she reused across multiple accounts. Without MFA, they were able to take control of her email, online banking, and social media.

Had Vero enabled MFA, the hackers would have needed additional factors, like a code sent to her phone number, which could have prevented access. This case shows why you should always turn on MFA and avoid using the same password for different accounts.

5 Common MFA Methods

Here are some authentication factors you can use for your added protection:

- **Physical token:** A small device that shows a one-time PIN.
- **Security key:** An electronic key that plugs into your device.
- **Biometrics:** Fingerprint, face, or iris recognition for secure access.
- **Authenticator app:** Mobile apps, such as Google Authenticator, that generate one-time codes.
- **SMS, email, or voice call:** A random code sent to you to verify your login.

For more information, visit https://www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication