PASSWORD SECURITY TIPS



Use Strong Passwords & Implement MFA: Use complex and unique passwords for all your important accounts and systems. Implement Multi-Factor Authentication (MFA) wherever it is supported.

Change Passwords Regularly: Update passwords periodically, especially for critical accounts. Every 90 days is a good frequency.

Use Complex Passwords: Combine uppercase and lowercase characters, numeric, and special characters. For example, "**ILmbWcSAMS!@#231**".

Consider Using a Password Manager: Password managers help store and generate strong passwords for different accounts. Choose a reputable password manager.

Do Not Reuse Passwords: Each account should have a unique password to prevent multiple accounts from being compromised if your password is compromised.

Password Length is Important: Ensure that your password is at least 14 characters long. An 8 character password can be hacked in a few hours with modern computing systems.

Avoid Common Passwords: Don't use easily guessable passwords such as "**password**", "**password123**", "**qwerty**", or "**123456**." In 2022, "**password**" was the most used password in the world, followed by "**123456**". We must do better.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time