Cybersecurity Basics

Identify

Know what you need to protect.

→ Identify and document endpoints that store your sensitive data (phones, tablets, and computers) as well as the cloud services that hold your sensitive data (email, financial websites, backup and cloud services).

Protect

Secure your endpoints with adequate protections.

→ Enable a password, a screen saver lock screen, and encryption to protect against unauthorized access when not in use or due to theft.

Secure the locations that store your sensitive data.

→ Enable multi-factor authentication (MFA) on all accounts where available (email, banking websites, data backup services). For additional protection, use an authenticator app instead of a text message for MFA.

→ Implement email filtering to protect from email phishing attacks designed to trick you into providing your sensitive information.

Update or remove software regularly.

→ Operating system security updates and installed software updates should be applied regularly to fix newly discovered vulnerabilities. Remove outdated or unnecessary software to minimize vulnerabilities.

Use unique and complex passwords for each account.

→ Unique and complex passwords should be used for each account to protect against automated attacks that can try thousands of password variations per minute from gaining unauthorized access. Use a reputable password manager such as LastPass or 1Password to securely manage and organize your unique and complex passwords.

Recover

Back up critical data.

→ Equipment failure, cyber-attack, and physical theft can cause data loss. Protect critical data by implementing regular automated backups.

D3 NETWORKS
A member of the CISSP Certified Cybersecurity Professionals Network

415-789-4077
hello@d3networks.net