

Cyber Security Safety Tips

How to Spot Phishing

The screenshot shows an email interface with the following elements and annotations:

- Sender:** David Martin (Dmartin@socoastauditing.com). Annotation: "The email is unexpected and comes from an unknown sender." (with a red arrow pointing to the sender name).
- Subject:** SharePoint Attachments. Annotation: "The email requests quick action" (with a red arrow pointing to the subject).
- Text:** Expires April 19, 2018. (with a red arrow pointing to the expiration date).
- Text:** Private and Confidential. Qualcomm Contract Approval. (with a red arrow pointing to the text).
- Link:** Review Document. Annotation: "The email asks you to either click on a link, download a document or provide sensitive data, such as your username/password" (with a red arrow pointing to the link).
- Footer:** David Martin uses SharePoint to share documents securely. [Learn More.](#)

How to Stop Ransomware

- Don't click on links or open attachments in suspicious emails.
- Backup regularly. You won't need to pay a ransom for files you have backed up.
- Keep the backup disconnected from your system.
 - Ransomware encrypts whatever drives or shares that are connected to the infected system.
- Keep software up to date.
- Set your antivirus and anti-malware software to scan and update automatically.
- Report any ransomware incident to the local:
 - FBI field office
 - US Secret Service field office

Protect Your Identity on Social Media

- Know your social media contacts (including LinkedIn contacts).
- Set your security and privacy settings to the level of your comfort for personal data exposure.
- Don't post on social media:
 - Vacation or personal plans
 - Your full birthdate
 - Information on your children
 - Information on new purchases, such as jewelry, cars, or electronics

Have Strong Passwords

- Have a unique password for every account
 - Don't use variants of other passwords
- Passwords should be at least 12-14 characters in length
- Avoid using:
 - Common names, such as the names of your family members, pets, movie characters, or car models
 - Words that can be found in any dictionary
 - Common keyboard combinations such as adjacent letters and sequential numbers

Protect Your Important Accounts

- Always use two-factor authentication when possible.
- Check your account history for unexpected usage
- Never provide account passwords or login information to anyone

Additional Resource - 101 Data Protection Tips:

<https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe#Online>