

Tip 1: Social Engineering Awareness

- Be cautious about sharing personal details with strangers, whether online or offline.

Share your strategies for identifying and avoiding social engineering tactics.


Tip 2: Secure Wi-Fi Networks

- Only connect to secure and trusted Wi-Fi networks.

Public Wi-Fi can be risky

Share, how do you ensure your Wi-Fi connections are safe?

Tip 3: Strong Passwords

- The first line of defense! 
Use unique, complex
passwords for all your
accounts.

Share your favorite tips for
creating and managing
passwords below!

Tip 4: Two-Factor Authentication (2FA)

- An extra layer of security!
Enable 2FA wherever possible.

Who here has turned on 2FA,
and what's been your
experience?

Tip 5: Phishing Awareness

- Don't take the bait! 🐟 Be vigilant against phishing emails and suspicious links.

Share stories or tools you use to spot phishing attempts!

Tip 6: Software Updates:

- Stay current! Regularly update your software and apps.

Tip 7: Privacy Settings

- Guard your data! Review your social media and app privacy settings.

Have you made any recent adjustments?

Tip 8: Device Security

- Secure your devices with passwords or biometric authentication.

Do you have any device security tips to share?

Tip 9: Email Encryption

- Consider using encrypted email services to protect sensitive information in your emails.

Have you explored any secure email options?

Tip 10: Educate Yourself

- Stay informed about the latest cybersecurity threats and best practices.

Are there any cybersecurity blogs, podcasts, or news sources you follow?

- **SHARE YOUR PERSONAL EXPERIENCES, INSIGHTS, OR ADDITIONAL TIPS FOR STAYING SECURE ONLINE**