Protecting Your Personal Information Online

Strong Passwords

- More sensitive accounts require stronger passwords
- The longer the better
- Use familiar sentences, like a line from a song or book

Spam & Phishing

- Spam is unwanted email sent by strangers
- Marking spam as “junk” or “spam” allows filters to recognize similar messages as spam and send them directly to your spam folder
- Phishing is an attempt to steal someone’s identity via email or website
- Smishing is phishing via sms (text) messages
- Do not open links in an email or text you find suspicious
- Forwarding suspicious texts to 7726 (“SPAM”) for free
- Tips from the FTC: onguardonline.gov

Telltale Signs of Phishing

- Strange links embedded in emails, texts, or unfamiliar websites
- Requests for personal information & obvious typos or errors
- Emails or texts that create a sense of urgency

Shop Securely Online

- Always look for the “S” in “https” and the lock symbol

Best Practices for Social Media

- Never give out sensitive information over social media
- Adjust your privacy settings
- Avoid linking different social media accounts
- Always log out when using a public computer or public WiFi