Security Online

Terminology . . . so we are all on the same page

Spam: unwanted message or text

Phishing scam: an illegal practice involving emails or texts that claim to be reputable organizations, designed to get you to reveal personal information such as passwords and credit card information. Some have links that will allow access to your computer or smart device.

Ransomware: malicious software that blocks access to a computer or network until some amount of money is paid. Ransomware attacks both individuals and businesses.

Malware: software that interferes, damages or has unapproved access to your computer.

Virus: a computer code capable of causing damage to data and software.

Important item: Stay updated with your computer software, especially your operating system and browsers.

Use a browser with built-in security features, such as Google Chrome, Mozilla Firefox, or Mac Safari.

Use websites that have encryption to protect your information. Look for the lock icon or the s in https://

Use strong passwords. Avoid using the same password for multiple accounts. Use a variety of letters, numbers, and keyboard characters.

Use two-factor authentication, especially for financial site.

bob.goode@stlgs.org

Have a good anti-virus application and malware application. Keep them up-to-date.

Be careful what personal information you share online.

Be careful doing any financial information while traveling. If you must do so, then use a virtual private network (VPN). Use caution if you select to use a VPN application. Some are spyware.

An alternative to VPN is using your phone hotspot. However, it can drain the battery and uses network data.

QR Codes (Quick Response): very convenient bar codes that can direct you to store coupons, websites, and landing pages. Be leary of third-party QR codes or an unsolicated ad with a QR Code.

Phishing: an email that looks like it comes from a legitimate source seeking information from you. Click on the little triangle immediately after the sender to find the actual sender's email address.

Banks and other businesses do not send emails or text messages asking you to login. Go to the actual site instead of clicking on links in an email.

Be careful opening files in emails.

Do not click on the STOP link in emails. This just tells the spammer that your email is active.

We used "Be Careful" several times. You can still enjoy being online. Just (your guessed it) be careful.

bob.goode@stlgs.org