HOW TO STAY SAFE ONLINE?

BASIC DIGITAL SAFETY

1 PASSWORD & SECURITY

Using strong, unique passwords for each account and employment of password managers to securely store them. Multi-factor authentication should be enabled to provide extra protection.

2 SCAMS & PHISHING

Recognize and avoid phishing emails, texts, or websites that phish for personal information. One should always verify the sender and be very careful while clicking on links or downloading attachments.

3 DATA ENCRYPTION

Ensuring data security through encryption tools for emails, files, and communications over the web to ensure that any form of interception might be difficult to handle without access by unauthorized parties.

4 SAFE BROWSING PRACTICES

Not accessing sites that have malware, checking a website for HTTPS to ensure it encrypts communication, and the use of browsers or add-ons focused on privacy, like VPNs.

5 SOCIAL MEDIA PRIVACY SETTINGS

Changing the privacy settings on social networking sites to include options on who can view your information and posts. Being cautious with what one posts online, so as not to invite identity theft or personal.The FTC provides detailed information on online privacy, including tips on managing privacy settings and safeguarding personal information.

reference: www.consumer.ftc.gov