Tips and Tricks to Staying Safe on the Internet

1. Your bank or co-op will never ask for information they already have, such as your bank account or bank routing numbers. When in doubt, call them!

2. Make sure to create a safe password for your accounts. Use a combination of letters, numbers, and special characters to create complex passwords (the longer the password the better!). You may use a password keeper to remember your passwords.

3. Restrict Wi-Fi usage when traveling. Only use Wi-Fi in secure places where you trust the network or use a VPN.

4. Update your software! This includes Microsoft Word, web browsers (Safari, Chrome, Internet Explorer, etc.), and Adobe Reader.

5. Back up all your files! This will help so you do not lose important documents if you were ever to be locked out. Store the backup in a safe place in case of natural disasters.

How to Protect Yourself

- **Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.**

- **Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing), and call the company to ask if the request is legitimate.**

- **Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.**

- **Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.**

- **Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.**

- **Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.**

- **Be especially wary if the requestor is pressing you to act quickly.**

This information comes to you from FBI.gov.
You can learn more about what to do regarding scams on their website:
https://tinyurl.com/jyh47383