10 Ten Tips to Avoid Cyber Fraud:

1. Be cautious of emails that contain attached files; the files may contain viruses.
2. Avoid filling out forms contained in email messages that ask for personal information.
3. Do not reply to unsolicited (spam) email or pop-up messages that ask for personal or financial information.
4. Do not click on links in an unsolicited email.
5. If you receive an email claiming to be from a company you do business with, contact the business to verify that the email is genuine.
6. Log on directly to the official website for the business identified in the email instead of clicking a link in an unsolicited email.
7. If an email appears to be from your bank or credit union, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information. Financial institutions will not request your personal information via email.
8. Wi-Fi hotspots provide free Internet access, are often in coffee shops, libraries, airports, hotels, universities, and other public places. While convenient, public Wi-Fi networks often are not secure. Protect your personal information while using public wireless networks.
9. Avoid exposing sensitive information such as your logins, passwords and your Social Security number.
10. If a Wi-Fi hotspot does not require a password, it is not secure. Other users on the network can see what you send. Your personal information, private documents, even login credentials could be accessed without your knowledge or permission.