November 2020 Security Newsletter
Do not Click That Link!

The 2020 election cycle has generated a flood of text messages from people interested in connecting with you. Some are legitimate organizations. Some are scammers trying to steal your money.

Scammers may pose as an organization seeking your support for a candidate or an issue. Their computer-driven systems automatically send text messages to thousands of mobile phones. Those messages will ask you to support their cause or their candidates in convincing terms. The message will ask you to click a link to be taken to a website where you can learn more or sign up to help.

Those websites will ask for your information: name, email address, home address, date of birth, and whatever other information they can convince you to give them. They will then use your personal information to steal your identity, your good reputation, and your money.

There is a simple solution to this problem: Do not click on any link in any unexpected text from anyone you do not know. Simply delete the text message.

The same advice goes for any email message you may receive.

Scammers will soon use the holiday shopping season to do the same thing: they will try to convince you to give your information which they will use to steal from you. They will offer great deals on the season's hottest items that you want to give as a Christmas gift. Just ignore unexpected emails from strangers. They may use kind words to persuade you to fall into their trap. But they are just thieves.

Remember your mom's advice when you were a kid: Do not talk to strangers!