SUMMARY OF SUGGESTIONS FOR SCAM AND CRIME PROTECTION

EMAIL

1. Opening an email is OK. However, bad things can occur with the attachments and links. Attachments that end in **.exe are particularly dangerous.**
2. Be careful with emails even from people you know. **Email spoofing** is where someone--usually for malicious purposes--sends an email that looks like it is from a source you know like a friend or bank. The email is **not** from the source shown on the email.
3. Beware of an email that has strange language and incorrect grammar, even if it looks like it maybe from a source you know.
4. Delete emails that look like they come from banks, credit card companies, Internet servers, telephone companies, etc. saying you have a problem and need to "click here" to login--these are really bad!
5. Delete emails from someone claiming to give you huge amounts of money if you help them transfer money--the classic Nigerian scam. These are dangerous.
6. It is probably a good idea not to put anything on an email that you would not want the whole world to see.
7. Delete an email that comes from a friend or relative claiming to be in trouble while traveling and asking you to send money.
8. Use "Bcc" instead of "Cc" or "To" when sending an email to lots of people--like a holiday greetings.

IDENTITY THEFT PROTECTION AND SCAMS

1. Get Identity protection from one (you only need one) of the national credit bureaus--Equifax, Experian or TransUnion--or other reliable companies. Be sure to get Social Security number monitoring and Credit Report Lock.
2. Check bank and credit accounts often. Also check IRA, 401ks, stocks and other investments.
3. If possible use a separate computer for banking and financial transactions only. One that you do not use for emails, Internet searches etc.
4. Don't store personal information like Social Security numbers, credit card numbers or drivers license numbers anywhere on computers.
5. Keep personal information like birth dates, mother's maiden name, address etc. off of social media sites such as Twitter, Facebook and various forums.

CRIME PROTECTION

1. If you leave a car in the driveway or street curb at night, take out the garage door opener.
2. It is best not to open your front door to strangers. Talk through the door or install an intercom.
3. Have a locked mailbox. Tax time is popular for mail box thieves.

4. Immediately hang up if a caller says they are from the IRS, law enforcement, electric power company, etc. wanting you to send money due to some problem.
5. Beware of a phone call from someone claiming to be a relative like a grandchild who is in trouble and needs you to wire money.
6. Shred documents with personal information such as pre-approved credit notices.
7. Keep doors and windows locked even when at home. There are many cases of burglars entering homes when residents are inside.
8. Beware of young people coming to the door trying to sell magazines for some charity or school function. They may even claim to be neighbors. Even though some of these maybe real magazine sales people, they over charge and lie about the charity--sleazy at best crooked at worst.

"If it looks like a Phish, swims like a Phish and smells like a Phish it is probably a Phish"