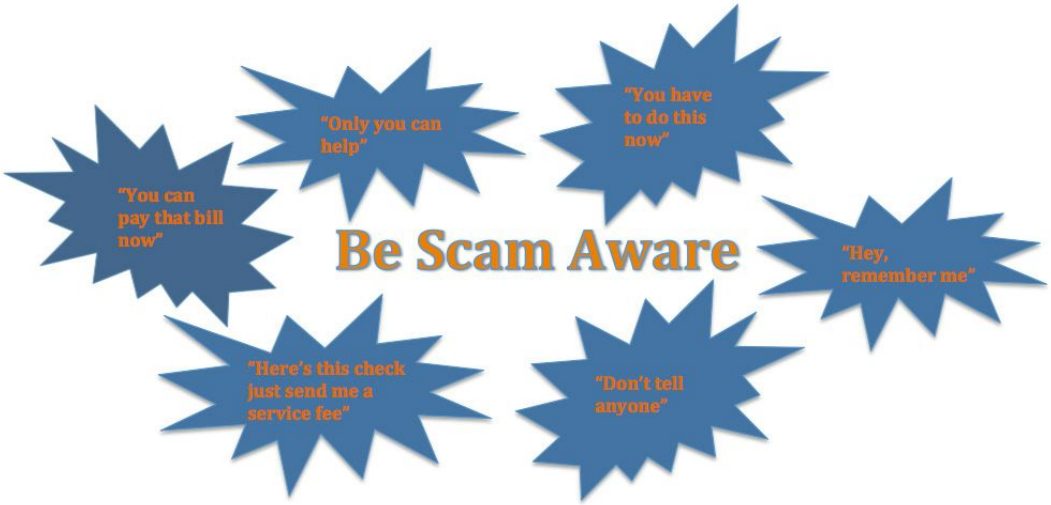
**Be Scam Aware - stay safe online and beyond ….**

As part of the National Cyber Security Awareness month we've been focusing on tips to help you practice safe computing.

Tip #4: BE SCAM AWARE!

These tips can be applied for your online security and other situations as well.

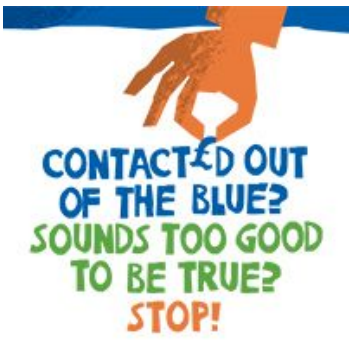
**Be SCAM AWARE regarding any activity that you didn't initiate.**




**If you make the call or initiate contact, you are probably safe. If, on the other hand, someone contacts you be on the alert for a scam.**

If someone contacts you by email, web (facebook, twitter, dating accounts, etc.), phone, or even in person --- be very, very careful! BE SCAM AWARE: Don't give people any personal information unless you are 100% sure who they are! REMEMBER: You can always suggest being in touch again in ways that ensure identification.

**A few specific examples:**




1) A person contacts you on facebook with something like "hey remember me --- we talked a couple months ago about this great opportunity." BE AWARE: Great opportunities rarely come your way from facebook, email, chat rooms, etc. REMEMBER: Facebook and most other online services offer no real identity protections. Anyone can get an account claiming to be anyone!

2) Someone comes to your home and offers to do work on your property for a discounted rate. BE AWARE: Deals that require immediate decisions or that seem too good to be true are almost always scams. REMEMBER: Take time to research the credibility of the companies that provide the services you need.

3) You go to a website looking for a recipe and something pops up to alert you that your computer needs attention and to install a "free" application to fix it. BE AWARE: Only trust software from the people you trust! REMEMBER: Nothing is "free"!

4) You get a call from a charge card company (or any other bill including the IRS) and they say you are behind on your payment. They would be happy to help you clear that up immediately and/or if you don't pay something bad will happen. BE AWARE: Only give financial data to companies when you have made the call to the bill pay phone number listed on the official bill. REMEMBER: Anyone can claim to be anyone on the phone (or online, in email, on facebook etc.)!


5) You get a phone call, email, or other message from a "relative" (grandchild, niece, nephew,etc.) and they claim to be in trouble and need money. BE AWARE: Requests for immediate money are almost always a scam. REMEMBER: There is always help available in every state and in every country so ask other people you trust to find out the details.

6) You meet someone online and they seem great. They seem really nice and they seem really interested in you. They begin are asking you for personal information and/or want to meet you in person someplace "quiet" or "private". BE AWARE: Don't allow yourself to be alone with someone you met "online" and do not share personal information or photos with them! REMEMBER: There are always public places to meet.

7) You like that new app on your phone which allows your friends to see where you are. BE AWARE: If your friends can see that information, others who are less than friendly are able to see it too. REMEMBER: Always understand the privacy rules for the apps and online services you use. Make those rules as restrictive as possible for your accounts.

**You should ALWAYS SUSPECT a SCAM ---**

- **if you are being pressured to make an immediate decision**
- **if the deal seems to good to be true**
- **if you are being asked to provide money or personal information for any reason to someone you can't identify and/or a situation you have no way to verify**

**Additional resources:**

https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf
http://stopthinkconnect.org/
https://www.staysafeonline.org/