Be Safe Online – Don't Be A Victim

Avoiding Scams, Malware & Phishing

Scams, hacking, malware, viruses, & phishing are all about money. They are the actions of big business and are not just random things that happen to people. They are all parts in an industry that makes a tremendous amount of money. They gather information through trickery, theft and mining the information that we thoughtlessly place on the internet. The information is then held for ransom or sold to other criminals that use it to perform other illegal activities.

How do you avoid falling victim to scams, malware and phishing?

You start by setting up a solid defense against these threats, then you must be careful about the software that you install on your computers, how you use your computers and the information that you provide to others.

Solid Defense

For a solid defense, see our Standard Recommendations document for how to setup your computer and network to operate more securely.

Avoid downloading software that you don't want:

- **Download programs only from websites you trust.** If you are not sure whether to trust a program, enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware. Files that end in the extensions .exe or .scr commonly hide malware. However, even files with familiar extensions such as .docx, .xlsx, and .pdf can be dangerous.
- **Pay Attention & Read all security warnings, license agreements, and privacy statements** associated with any software you download. Before you install something, consider the risks and benefits of installing it. Even many reputable programs tell you that they are about to install additional software to "help" you, but it is usually software that you do not really need and often are programs that either spy on your behavior or lead to virus programs later.
- **Never click "Agree" or "OK" to close a window.** Instead, click the red "x" in the corner of the window or press Alt + F4 on your keyboard to close a window.
- **Be Afraid of "free" things.** Such as "free" music and movie file-sharing programs, and be sure you understand all of the software that is packaged with those programs.
- **Don't click links on suspicious websites or in email messages.** Instead, type the website address directly into your browser, or use bookmarks.
- **Don't automatically trust** that instant messages, email messages, or messages on social networking websites are from the person they appear to be from. Even if they are from someone you know, contact the person before you click the link to ensure that they intended to send it.
- **Ask someone who knows.** If you are not sure about a strange message or a program, then ask someone that you trust.

Email Safety

See our "Standard Recommendations" or "10 Email Safety Tips" documents for how to use your email more securely.

Computer Safety

See our Standard Recommendations document for suggestions on how to safely use your computer.

Mobile Safety

- Screen Lock Code
- Security App
- Mobile Device Management App
- Be careful about the information you provide when using your phone, tablet or laptop in a public setting. People can see what you are typing and hear what you are saying.

Phone Scams

- Most phone scammers are very high pressure and quite convincing. Do not give in to their tricks.
- Do not give personal or private information to someone who called you
- Do not give your credit card number to someone who called you
- Microsoft will not call you
- The IRS will not call you
- Be suspicious of anyone that calls you unexpectedly
- Random people do not call you to tell you that your computer is infected with a virus
- Do not give out passwords or other personal information over the phone
- If you have an error message with a phone number, do not call it
- If someone calls you, a good way to check them out is to call the main contact number on the company's website and ask for that person.
- Some of the questions that they ask may seem harmless like "do you shop online", "do you have any pets" or "how old are you", but these are classic phishing questions they use to gather more information about you and get you comfortable answering questions.

What To Do

Be paranoid. If something on your computer or the person on the phone doesn't seem right, then it probably isn't. Always verify before clicking a link, installing a program or giving out information.

If you think you have been hacked or have a virus, stop what you are doing and call your computer support person or someone who is knowledgeable about computer security immediately. The longer you use your computer after a virus or hack happens, the more difficult it is to remove the damage.

If you have given out your credit card number and are concerned about it, then call your credit card company to check your account and possibly put a fraud alert on the account. If there is already fraudulent activity on your card, then the best thing is to cancel the card and have a new one issued.

If you think one of your online accounts has been hacked, change the password and security questions. Verify what email accounts are allowed to reset the password. Sometimes hackers will insert their information into your account settings, so they will be notified of the password change or to block you from resetting the password.

If you need help or have questions about internet security, contact us using the information below.

We are The Technology Service Provider for Housing Authorities!

Let Us Start Helping You!