ELECTRONIC DEVICE SECURITY

Reduce the risk of data breaches at home & on the go.

Electronic devices are indispensable parts of our lives. We use them for business, banking, socializing, shopping and much more, meaning there's plenty of information stored in the programs and websites we visit most often. Because of this, computers and smartphones can be treasure troves for identity thieves and scammers seeking to infiltrate your system.

General Computer Security

Performing a few simple maintenance tasks can offer protection from common problems like hackers, spyware, trojans, viruses, and worms.

Stay up-to-date with device protection:

- Install a good antivirus and anti-spyware program, and regularly update them.
- Use an active firewall on your computer and router and recognize any changes.
- Update your software regularly, and set your software to download updates automatically if possible. Using updated software helps to secure your device threats. With new updates, security features are added and "bugs" are squashed.

Be mindful of your actions online:

- Avoid suspicious sites altogether.
- Do not download programs from the Internet without being certain you really want the program and that you trust the company or person from which it originates. Also, always ensure that your antivirus program is working and up-to-date before downloading any files from the web.

Know what is normal:

- Always be aware of changes in your computer. If it suddenly slows down for more than a few seconds, there may be something running in the background. If it happens more than once or twice and does not seem to be related to a program you are running, do a full scan with an anti-virus program, or take your device in to be looked at by a professional.

When you are done using your computer:

- Turn it off or disconnect it from the network. Many virus-like programs attack while your computer is in sleep mode. The hackers depend on you leaving your computer turned on to be available to them.
- If you do decide to keep your computer on when not in use, make sure it is locked with a secure password. This helps protect you from unauthorized user access.
- Set up a timeout. Choosing a set time for your device to enter "sleep mode" can prevent others from continuing your online banking session if you left your computer unattended without logging out. You can set this timeout period by visiting your device's settings.

What is a virus?

A virus is a man-made computer program that, when opened, infects your computer and attempts to spread itself to other computers. It will often attempt to spread via e-mail automatically by sending copies of itself to everyone in your address book.

What is a worm?

A worm shares most of the traits of a virus, but is able to spread on its own without human interaction.

How do they spread?

Viruses are mainly spread via e-mail, although some websites can infect your computer as well. Worms seek out non-infected computers by searching the network, and then spread themselves by exploiting security weaknesses.

Computer users often install viruses on their computers by accident. Because viruses spread themselves automatically, they often come from friends or family members without their knowledge. Even though an email came from someone you trust, you may still be in danger of contracting a virus. Even if a message comes from a sender you know, be weary if it contains a headline or misspellings that seem unusual, links, or attachments. This may be a virus impersonating the sender.

If someone you know sends you an attachment, scan it with an anti-virus program before you open it. Do not click on suspicious attachments or links.

How do I protect myself and my computer?

- Keep anti-virus software up-to-date so that is able to tackle the newest types of threats to your system.
- Set your anti-virus program to scan at start-up.
- Set your anti-virus program to scan each and every file when it's used by the computer.
- Keep your computer software up-to-date -- both your operating system and applications (even games) that you use!
- Be very careful when using peer-to-peer file sharing programs, viruses are easily spread on these types of services.
- Make sure to scan all downloads with an anti-virus program before installing.
- Don't install any software or programs unless they are from a source you trust.

Just in case:

Don't forget to regularly back up all of your important files. If you do happen to get a virus, even after following all of these helpful tips, you may need to do a system reset on your device to remove a virus. Backing up files ensures your important documents will not be lost if this must be done.