**subject line: are your online behaviors putting you at risk?**

**Many online behaviors put users at risk.**

Most of us use the internet as we need to, without a lot of thought about our computer and personal information being “safe” while online, whether it be for work or pleasure.

In fact, a recent survey1 indicated that almost a third of American internet users don’t have, or don’t know if they have; anti-virus, anti-malware, or anti-spyware software on their computer.

This indicates a lot of people take being safe while using the internet for granted. Unfortunately, nothing could be further from the truth. According to the FBI’s most recent information, the FBI is receiving an average of more than 800 calls per day relating to cyber-crime. And in 2016, there were verifiable victim losses due to cyber-crime totaling $1.33 billion.

**What About Using A Public WiFi System?**

Unless you have up to date anti-virus, anti-malware, or anti-spyware software on your computer, it is not a good idea to use a public WiFi system.

**How To Protect Your Computer**

Considering the safety issues with using the internet and WiFi systems, it is important you know the necessary steps to take and stay safe while on the internet. According to the FBI, the following safety tips will help protect your computer from intrusion: **Keep Your Firewall Turned On:** A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information.

**Install or Update Your Antivirus Software:** Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it.

**Install or Update Your Antispyware Technology:** Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code.

**Keep Your Operating System Up to Date:** Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

**Be Careful What You Download: Carelessly:** downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don’t know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

**Turn Off Your Computer:** With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being “always on” renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker’s connection—be it spyware or a botnet that employs your computer’s resources to reach out to other unwitting users.

Warmly,

XXXXX

*1. From Allan Newman Research, a national opinion research firm.*