National Cyber Security Awareness Month, October 2017

Simple Steps to Online Safety

Keep a Clean Machine

- **Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option;
- **Protect all devices that connect to the Internet:** Along with computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information

- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.
- **Make your password a sentence:** A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music;"); On many sites, you can even use spaces!
- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.
- **Write it down and keep it safe:** Everyone can forget a password; Keep a list that's stored in a safe, secure place away from your computer. You can alternatively use a service like a password manager to keep track of your passwords.

Connect With Care

- **When in doubt, throw it out:** Links in emails, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- **Protect your $$:** When banking and shopping, check to be sure the site is security enabled. Look for web addresses with "https://" or "shttp://," which means the site takes extra measures to help secure your information; "Http://" is not secure.

Be Web Wise

- **Stay current.** Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.

- **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.
- **Back it up:** Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen

- **Safer for me, more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you.** The Golden Rule applies online as well.
- **Help the authorities fight cybercrime:** Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.

Own Your Online Presence

- **Personal information is like money. Value it. Protect it.:** Information about you, such as your purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites.
- **Be aware of what's being shared:** Set the privacy and security settings on web services and devices to your comfort level for information sharing; It's OK to limit how and with whom you share information.
- **Share with care:** Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it could be perceived now and in the future.

Acknowledgement: The Anti-Phishing Working Group (APWG) and National Cyber Security Alliance (NCSA) led the development of the STOP. THINK. CONNECT. campaign. The U.S. Department of Homeland Security provides the Federal Government's leadership for the STOP. THINK. CONNECT. campaign.