Investigator Insight

Personal Cyber Security

Insight and Tips for Becoming Cyber Aware

Through the efforts of multiple agencies, **National Cyber Security Awareness Month** is observed each October to help make consumers more cyber aware and, in turn, more secure digital citizens.

Here, from the Department of Homeland Security's Stop. Think.Connect. Campaign, are tips shared in an effort to "increase the understanding of cyber threats and empower the American public to be safer and more secure online." You likely have seen these tips over the last several months as we've shared ways to protect your personal identifiers when connecting to the internet and reduce the risk of identity theft.

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 available.
- Protect all devices that connect to the Internet: Along with computers, your smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.

Protect Your Personal Information

- Secure your accounts: Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- Unique account, unique password: Having separate passwords for every account helps to thwart cybercriminals.
- 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.
- Own your online presence: Set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Connect with Care

- When in doubt, throw it out: Links in email, tweets, posts and online advertising are often the ways cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email.
- 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 money: When banking and shopping, check to be sure the sites are security-enabled. Look for web addresses with "https://," 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, 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.

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.

Visit www.stopthinkconnect.org for more information.

A service of the Investigators of Kroll. These materials are derived from the research and discovery activities of Kroll Fraud Specialists and Licensed Investigators, and have been gathered from personal, historical, and aggregated experience performing specialized restoration services on behalf of Identity Theft victims. While believed to be accurate, these materials do not constitute legal advice, and are not guaranteed to be correct, complete or up-to-date. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the express written consent of Kroll. These materials are provided for informational purposes only.