IDShield | INVESTIGATOR TIPS

Responsible Cyber Citizens Are Key to a Safer, More Secure Online World

According to Internet World Stats, more than half of the world's population uses the internet. Who is responsible for keeping all of these users safe as they work, bank, shop, and communicate online? Everyone! That's the message from the National Cyber Security Alliance (NCSA) as it promotes National Cyber Security Awareness Month (NCSAM) throughout October.

NCSAM is in its 14th year of educating consumers of all ages, and businesses of all sizes and types, about online safety. Since 2010, the annual awareness campaign has asked digital users to Stop. Think. Connect.™ as follows:

STOP: make sure security measures are in place.

THINK: about the consequences of your online actions.

CONNECT: and enjoy the internet.

This year, we're reminded that an individual's online actions can strengthen or imperil the safety and security of all users. That may sound intimidating, especially if you don't consider yourself very tech-savvy. But the NCSA has identified seven simple steps that we can all take to better protect ourselves as well as our fellow netizens:

1. Lock down your login: NCSA recommends providing an extra layer of security by using "strong authentication" – also referred to as two-factor (2FA) authentication – to protect your online accounts with the most sensitive information such as email, banking and other financial accounts, and social media. You can find out which online services support 2FA here.
2. Keep a clean machine: No, this doesn't mean wiping the fingerprints off your screen or keeping crumbs out of the keyboard (although those are both good ideas). It means keeping all software on internet-connected devices up-to-date. Why is this important? Besides offering the latest features, updates often include bug fixes and security updates to patch vulnerabilities that could allow unauthorized access to certain accounts and personal information.
3. When in doubt, throw it out: Delete, and don't respond to, emails, texts, tweets, and social media posts with suspicious links. Even if the message looks legitimate and seems to come from someone you know, be careful; hackers are really good at making phishing attempts look like the real thing, hoping you'll click on the link that can give them access to your personal information or infect your computer with a virus.
4. Back it up: Make a copy of your important files, photos and other information and store the copy safely.
5. Own your online presence: You don't have to overshare. Check the privacy and security settings on your apps and online accounts and adjust according to your comfort level.

6. Share with care: Think twice before you post a photo, a snarky comment about your boss, or unkind words about someone you don't even know. What you say and post online can affect you and others now and in the future as even deleted posts can remain on servers for years to come.

7. Personal information is like money: You wouldn't leave wads of cash lying around, free for the taking. Think about your personal information the same way: be careful about where, and with whom, you share it.

It's unrealistic to expect every online user to follow all of these steps every day. That's why IDShield looks out for members, monitoring your personal information, alerting you if any information appears to be compromised, and providing advice on what you should do to avoid becoming a victim of identity theft.

Kroll

A service of the Investigators of Kroll. 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.

2017-10-19