Remember These Top 8 Cyber Security Practices

1. Protect Your Personal Information. It's Valuable.

Identity theft risk can be minimized when online by not giving out personal information-your name, email address, account numbers, or Social Security number-until you know how it's going to be used, and who you are giving it to. Don't reply or click on any link in an unsolicited email or pop-up message asking for personal information.

Shopping Online. Be careful what personal information you give, and always make sure vendors have taken measures to secure their sites, indicators are a lit lock icon on the browser's status bar and a website URL that begins with "https" (the "s" stands for secure").

2. Know Who You Are Dealing With Online.

Always check out sellers before you buy. Legitimate businesses or individual sellers should give you a physical address and a working telephone number.

Phishing. These are unsolicited emails or pop-up messages claiming to be from businesses or organizations that you might be familiar with, like a bank or a major retail brand. The message will say that you need to "update" or "validate" your account information. Don't take the bait. Don't open unsolicited or unknown emails, don't download attachments from people you don't know or don't expect, and never reply to or click links in emails or popups asking for personal information.

Free Software and File Sharing. Downloading file sharing software is not advisable and not worth the risk. Online file-sharing can give people access to a wealth of information. If you don't check the proper settings while file sharing, you could allow access to files containing important personal information Be sure to read the End User License Agreement too, to make sure you're sharing files legally.

Spyware comes with many free downloads. This is software that is installed without your knowledge that adversely affects your computer, and may access your personal information. Resist installing any software unless you know exactly what it is. Install anti-spyware software and keep it up to date.

Email Attachments and Links. Many viruses sent over email or Instant Messenger won't steal your information or damage your computer without your participation. For example, you would have to open an email or attachment that includes a virus or a link to a site that is programmed to infect your computer. Don't open an email attachment unless you are expecting it or know what it contains.

3. Use Anti-virus Software, A Firewall, And Anti-spyware Software To Help Keep Your Computer Safe And Secure.

It's just common sense. An ounce of prevention is worth a pound of cure

Anti-Virus Software protects your computer from viruses that destroy data, cause crashes,or even steal your personal information It works by scanning your computer and incoming email for viruses, and deleting them. Your anti-virus software must be updated regularly. Most include automatic update features.

Firewalls help keep hackers from accessing your computer to gather information without your permission. Think of it as a guard, watching for intruders. For firewalls to work, they need to be configured properly and updated regularly. Some operating systems come with firewalls, but need to be turned on in order to work.

Anti-Spyware Software protects your computer from malicious spyware that monitors your online activities and collects personal information while you surf the web. It works by periodically scanning your computer, and then gives you a chance to remove any spyware found. Just like anti-virus software, it is important to regularly update your anti-spyware software to protect you from the latest threats.

4. Update Your Operating System.

Set up your operating system and web browser software properly, and update them regularly. Hackers take advantage of unsecure browsers and operating systems. Lessen risk by changing the settings in your browser or operating system to maximize online security. Also, it is important to update your operating system with "patches" to close holes hackers could exploit. Most operating systems can be set up to automatically update.

5. Use Strong Passwords Or Strong Authentication Technology To Help Protect Yourself.

Criminals may try to figure out your passwords to gain access to your computer. You can make it tougher for them by using passwords that have at least eight characters and include numerals and symbols, changing passwords regularly and using different passwords for each account. To further increase security of your online identity and sensitive information, utilize two-factor authentication tools. Two-factor authentication is a combination of a password or PIN used along with a token, smart card, or a biometric device. Strong authentication can also be a behind-the-scenes identity-verification process, which uses various data to establish whether or not a user is genuine. Ask your bank, online retailers and ISPs if they use stronger authentication tools for more secure transactions.

6. Back Up Important Files.

No system is completely secure. If you have important files on your computer, back them up and store them in a secure place. Make sure you keep the original software in the event of a system crash.

7. Learn What To Do If Something Goes Wrong.

Unfortunately, there is no way to know for sure if your computer is infected with malicious code. Be aware of any unusual or unexpected computer behaviors. This could be an important sign of infection.

Hacked or Computer Viruses. If this happens to you, immediately unplug your Internet connection from your computer. Next scan your entire computer with fully updated anti-virus and anti-spyware software.

Internet Fraud-Identity Theft or Phishing. If a scammer takes advantage of you online in any way, report it to local law enforcement, and then to the Federal Trade Commission at www.ftc.gov. If you get a phishing email report it by forwarding the email to **spam@uce.gov**. To find out more on what to do if you're a victim of ID theft go to **www.consumer.gov/idtheft**.

8. Protect Your Children Online.

Children present unique security risks when online - not only do you have to keep them safe, but you have to protect their data on your computer. Simple steps will reduce threats children face while online. Keep your computer in a central and open location in your home. Discuss and set guidelines and rules for computer use. Implement parental control tools. Teach your children never to give out their personal information in chatrooms or bulletin boards. If your child is in immediate danger call your local police.

National Cyber Security Alliance

The **National Cyber Security Alliance (NCSA)** is the go-to resource for cyber security awareness and education for home users, small businesses, and education professionals. A public-private sector partnership, NCSA sponsors and partners include the Department of Homeland Security, Federal Trade Commission, Department of Commerce, and many private sector corporations.

Our mission is to increase awareness and help all Americans learn effective responses to pressing cyber security and safety issues. NCSA provides tools and resources to empower home users, small businesses, schools, colleges, and universities to stay safe online.

Look for our Stay Safe Online national awareness programs or visit us at **www.staysafeonline.org** for easy-to-understand information on how to improve your cyber security.