Be Cyber Secure this Holiday Season

Many people will turn to online shopping this holiday season. If you choose to shop online for gifts this year, be sure you keep your information secure. The Internet enables criminals to use multiple ways to steal your information. Be aware of the different online scams. There are several steps you can take to prevent your information from being compromised this shopping season. Below are tips from the Federal Trade Commission and U.S. Department of Homeland Security to keep your personal information safe this season.

Online Banking
- Avoid accessing your personal or bank accounts from a public computer or public Wi-Fi network. Cybercriminals can gain access to your accounts through public Wi-Fi.
- When paying a bill online or making an online donation, be sure that you type the website URL into your browser instead of clicking on a link or cutting and pasting it from the email.

Online Shopping
- Make sure the website address starts with “https”; the “s” stands for secure.
- Look for the padlock icon at the bottom of your browser, which indicates that the site uses encryption.
- Type new website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

Email Scams
As technology advances, so do tactics for cybercriminals trying to steal your information. Many use email methods to gain access to your information. Here is a list of common email scams to look out for in your inbox:
- Phishing attacks use email or malicious websites to collect personal and financial information or infect your machine with malware and viruses. Emails might look legitimate and can encourage people to click on a link or open an attachment.
- Imposter scams happen when you receive an email seemingly from a government official, family member, or friend requesting that you wire them money to pay taxes or fees.
- “You’ve Won” scams happen when you get an email telling you that you have won a prize, lottery, or sweepstakes. They tell you there is a fee or tax to pay for the prize and request your credit card or bank account information.

What To Do If Your Information Is Stolen

The U.S. Department of Homeland Security (DHS) provides an Internet Scams Tip Card with information on what to do in the event your information is stolen online. DHS also has additional tips on what to do during a cyberattack to limit damage in its cyberattack fact sheet.