Michigan Department of Attorney General

consumer education

Bill Schuette
Michigan Attorney General

ONLINE SAFETY

Staying connected 24/7 is convenient; however, it also opens users up to scammers, hackers, and identity thieves. When online, remember these two important rules: 1) Never email or text any financial or account information; 2) Look for httpS on every page you enter personal information.

BROWSERS

We access the Internet through browsers. No matter which one you use (Chrome, Internet Explorer, Firefox, Safari, or Opera, etc.) it's important to keep them up-to-date. Most browsers update automatically or prompt you to update them.

A browser that has not been updated leaves sensitive information vulnerable and susceptible to malware.

Pay attention to the domain name of any website you visit. This will help you *consider the source* by giving you information about who controls the website content. The domain name is usually located at the end of a web address.

- **.com** = commercial
- **.net** = network
- .**org** = organization
- .**edu** = educational
- .**gov** = government
- .**au** = Australia
- .**ca** = Canada
- .**uk** = United Kingdom

COMPUTER SECURITY

The following simple steps will help protect your computer from many types of malware.

1. Install security software from a reliable company and set it to update automatically;
2. Set your operating system and your web browser to update automatically;
3. Set your web browser's security setting to at least medium to detect unauthorized downloads;
4. Use a pop-up blocker;
5. Don't click on links in pop-ups;
6. Don't buy security software in response to unexpected calls or messages;
7. Don't click on links or open attachments in emails unless you know what they are, even if the emails seem to be from friends or family; and
8. Download software only from websites you know and trust.

TECH SUPPORT SCAM / CONSIDER THE SOURCE

Con artists try to break into your computer by calling you or through a pop-up saying they are from a company like Microsoft and need to "fix" your computer.

Listen for the following:

- Your computer has a virus or malware they can "fix" for a fee;
- You need to buy additional (bogus) security products; or
- They try to trick you into installing malware that will steal personal information from your computer.

SAFETY TIP

Another good practice is to back up your computer files. Protect anything valuable by storing a copy on a device other than your computer. That way if you have an issue with your computer, you won't lose your favorite photos and important documents.

You can back up your files with an external hard drive, flash drive, CD, DVD, or you can use an Internet-based cloud storage service.

EMAIL AND PASSWORDS

There are several things to remember when it comes to email safety:

- **NEVER** open an email from a sender you don't know;
- Don't open email attachments unless you know who sent it and what it is;
- Hover your mouse over links to see where you would be redirected;
- Be alert to scams (Emergency/Grandparent Scam, Lottery or Sweepstakes Scam, Nigerian Scam, Ransomware, and Investment Opportunities);
- Consider two email accounts. One you use with friends, family, and other trusted sources (online banking, shopping, etc.) and another for all other purposes; and
- Enable two-step authentication.

CREATE STRONG PASSWORDS

- Don't use the same password for multiple accounts;
- It should be hard to guess, but easy to remember;
- Don't use anything that you share on social media.

SECURE WEBSITES

- Only send personal information through a secure website.
- Look for http**S** (the S stands for secure) on every page you enter personal information, not just when you log on.

SECURE NETWORKS

HOME WI-FI

- Hide your network name;
- Change the router's pre-set name and password;
- Turn on router's encryption; and
- Restrict network access to specific devices.

PUBLIC WI-FI

- Use secure public Wi-Fi. Don't assume that a public Wi-Fi is secure. In fact, most are not.
- You can only be sure it is secure if it asks you to provide a WPA or a WPA2 password.
- If you're not sure, it is best to assume the network is not secure.
- Log out of all account.
- Best Practices: don't enter personal information when using public WI-FI.

OnGuard Online provides additional information on their website (www.ftc.gov/onguardonline).

ONLINE ACTIVITIES

BANKING

- Protect your answers to security questions required before logging into your account.

SHOPPING

- Know the return policy - who pays shipping and is there a restocking fee?
- Check out securely. Look for https!
- Pay by credit card.

Additional online shopping tips are available in OnGuard Online's "Be Smart Online" section of the website (www.onguardonline.gov/smartshopper).

SOCIAL MEDIA

- Be cautious about posting personal identifying information.
- Use privacy settings to restrict access.
- Manually managing location services on your phone.
- Arrange an in-person meeting with someone you've met online in a safe place, and bring a friend!

HELPFUL WEBSITES

Attorney General (www.mi.gov/ag)

Stop.Think.Connect (www.stopthinkconnect.org)

OnGuard Online (www.ftc.gov/onguardonline)

Federal Trade Commission (www.ftc.gov)

Following this advice will go a long way toward protecting all of your devices as well as yourself online. And, never forget to **CONSIDER THE SOURCE**!

An electronic copy of this handout is available through the QR code below or on our website (www.mi.gov/ce). While you're there, schedule a presentation (www.mi.gov/ce) for one of our other seminars.

For questions, contact Attorney General Bill Schuette's Consumer Programs team at 877-765-8388 or agcp@mi.gov.