consumer
education
Dana Nessel
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 http**S** on every page you enter personal information.

STOP. THINK. CONNECT.

ASK: Can what I'm posting or sending be used against me?

ASK: Is what I'm looking at from a legitimate source?

CREATE STRONG PASSWORDS

- Increase the length of your passwords rather than focus on random use of letters, numbers, and symbols.
- Don't use anything that you share on social media.
- Consider using a password manager.
- Most important, don't use the same password for multiple accounts.

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.

DEVICE 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.

These additional steps will help secure your mobile devices.

9. Set up a remote wipe option to wipe everything off your device if it is stolen.
10. Consider a find your device option if you are prone to misplacing your phone.
11. Download apps from only trusted sources.
12. Make sure your device is undiscoverable and Bluetooth is turned off when not in use.

TECH SUPPORT SCAM

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.

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;
- Pay attention to whether your email address has been compromised; and
- Enable two-step authentication.

SECURE NETWORKS

HOME WI-FI

- Turn encryption and firewall on.
- Change the administrator router's default passwords.
- Change the default name of network and turn broadcasting off.
- Restrict network access to specific devices.

FCC's Protecting Your Wireless Network

PUBLIC WI-FI

- Verify the exact name of the official Wi-Fi network to avoid connecting to a hacker's network.
- Don't share personal information over public Wi-Fi even if the network is encrypted.
- Don't allow your device to automatically connect to Wi-Fi networks.
- Look for http**S**.
- Log out of all accounts when done.
- Turn Wi-Fi off and "forget" the network. "Forget" is a feature on your mobile device that removes the network from your connection options and prevents your device from automatically connecting in the future.
- Best Practices: don't enter personal information when using public Wi-Fi or consider using a Virtual Private Network (VPN).

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

ONLINE ACTIVITIES

BANKING

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

SOCIAL MEDIA

- Be cautious about posting personal identifying information.
- Use privacy settings to restrict access.
- Manually managing location services on your phone.

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.

HELPFUL WEBSITES

Attorney General
(mi.gov/ag)

National Cyber Security Alliance
(staysafeonline.org)

Stop.Think.Connect
(stopthinkconnect.org)

Federal Trade Commission
(ftc.gov)

‘;--have i been pwned?
(haveibeenpwned.com)

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

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