



Keeping Michigan consumers safe and informed!

Attorney General Bill Schuette's CONSUMER EDUCATION

Halloween is not the only event that may spook you this month. October is National Cyber Security Awareness Month, and there is plenty to be frightened of in the cyberworld—so take this time to learn about cyber safety and how to protect yourself online.

Attorney General Bill Schuette's Consumer Protection team joins the U.S. Department of Homeland Security and the National Cyber Security Alliance to focus on consumers and their cybersecurity and safety and mark October as the month to highlight these important issues.

Cyber Security Awareness Month was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online. 2016 marks the 13th year to celebrate this month and the sixth anniversary of the STOP.THINK.CONNECT. Campaign, whose capstone concepts include: "Keep a Clean Machine," "Protect Your Personal Information," "Connect with Care," "Be Web Wise," "Be a Good Online Citizen," and "Own Your Online Presence."

These themes and others are the focus of Schuette's free Consumer Education Presentation, "Online Safety." We invite you to celebrate the month by scheduling a seminar in your community.

We offer three items for you to consider this month to keep you safe online: **Consider the Source**; **Consider Two-Step Authentication**; and **Consider Your Online Access and Activities**.





Consider the Source

Consider the source is the theme of our “Online Safety” presentation. Cybersecurity starts with you. When you are online, you should continually ask yourself, “who is really behind the email or website” and “what is their agenda”? This will help you make decisions that will keep you safe online.

It is best practice to pay attention to the domain name (e.g., .com, .net, .edu, .gov) of any website you visit. Considering this source will give you information about who controls the content. For example, a .gov domain denotes a government website, while a .com, .net, or .org are domain names that can be purchased and used by anyone.

Be aware of pop-ups. There are generally two types: advertising and scams. You are putting yourself at risk (more advertising and more scams) if you click on links in pop-ups. Especially look out for pop-ups, emails, or phone calls that appear to be from a company like Microsoft and need to “fix” your computer for a fee or with bogus security software that will install malware and infect your computer and steal your personal information. **Remember, consider the source!**

Finally, it’s true you should never open an email message from somebody you don’t know, but you also should not assume that because you know the source—a family member, friend, or association of which you are a member—that links or attachments they send you are safe. A friend’s computer may be infected or hijacked and sending you infected emails. If an email subject or re: line sounds odd, or you are not expecting the email, proceed with caution.

Consider Two-Step Authentication

Two-step, two-factor, or multi-factor authentication protects your online accounts by adding an extra step to your basic log-in procedure. Without it, you enter in your username and password, and you’re into your account—which is single-factor authentication. With it, you are required to provide an additional piece of information after you enter your password to get into your account—which is two-step or multiple-factor authentication. It adds an additional layer of protection to prevent unauthorized access to your accounts.

You probably already use multi-factor authentication in your everyday life. Think of charging a purchase on your credit card: you have to provide the card itself then you are also often prompted to key in your zip code; or, think of withdrawing money from an ATM (automatic teller machine)—only the correct combination of your debit card and PIN (personal identification number) will allow the transaction.

Other variations include entering your password online and then a service sends you text, email, or voicemail message with a unique string of numbers that you will need to enter to get access to your account. Whatever the method, multi-factor authentication is not impervious to all hackers, but it is one of the best ways to protect your sensitive online accounts.

So how do you get it?

STOP.THINK.CONNECT.org offers several [videos on how to add multi-factor authentication](#) to many popular websites and services.



Consider Your Online Access and Activities

How do you access the internet? At home on a secure connection? From a public, free Wi-Fi? How you access the internet should factor into what you do and which sites you visit when you are on the internet.

If you have wireless internet access at home, you need to take the following steps to make sure that your network is private:

1. Hide your network name.
2. Change your router's pre-set name and password.
3. Turn on your router's encryption feature.
4. Restrict network access to specific computers.

If you are not sure how to do any of these things, talk to your internet service provider or consult a trusted source like the [FTC's OnGuardOnline website](#).

Beware public Wi-Fi spots. Scammers use eavesdropping software to steal personal information on public Wi-Fi, so make sure before you log on, that the connection is secure—never assume that it is.

You can only be sure that a connection is secure if it asks you to provide a WPA or a WPA2 password to log on. And even if it does, it is important to remember that while on a public Wi-Fi, log out of all accounts when you are done; do not open multiple accounts at the same time; and never enter personal information. For more public Wi-Fi safety tips, [watch this video from the FTC](#).

Popular online activities include: banking, shopping, and social media. Consider the following best practices when engaging in any of these online activities:



Banking

- Protect your answers to security questions before logging onto your account.
- Use two-step authentication.
- Never access from public Wi-Fi.



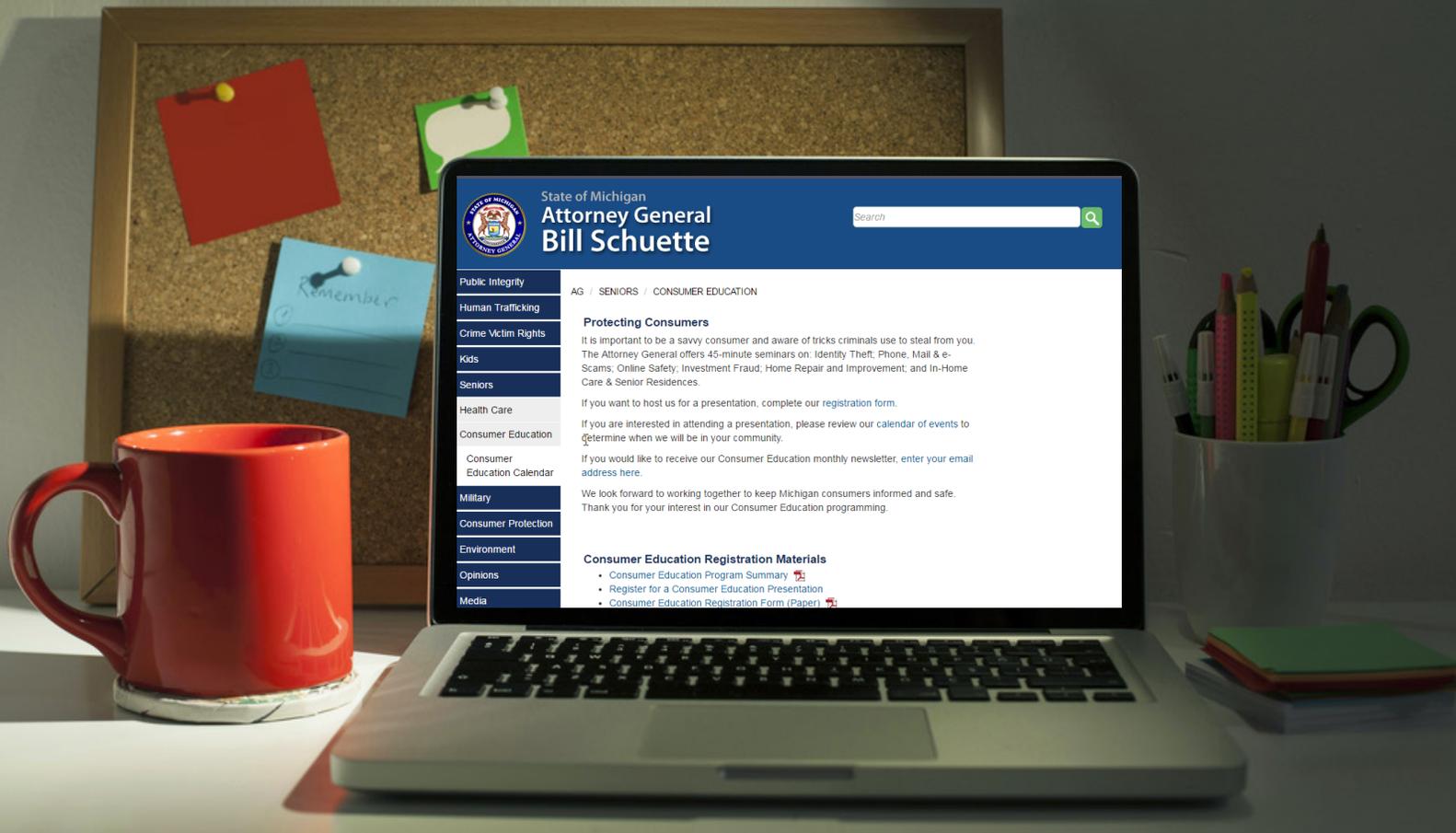
Shopping

- Look for "https" or the lock icon to make sure the site is secure.
- Pay by credit card.
- Know the return policy before you buy: who pays return shipping and is there a restocking fee?



Social Media

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



www.mi.gov/ce

Register for a Consumer Education Presentation

In addition to the Online Safety presentation, the Attorney General offers five other free Consumer Education Presentations that are available for your group, club or class.

Those topics include: Investment Fraud; Identity Theft; Home Repair & Improvement; Phone, Mail, & e-Scams; and In-Home Care & Senior Residences.

To register your site for a presentation, please complete the [online registration form](#).

CONNECT WITH US:

Department of Attorney General
P.O. Box 48909
Lansing, MI 48933
877-765-8388
[Email \(agcp@mi.gov\)](mailto:agcp@mi.gov)



Bill Schuette
Attorney General