MICHIGAN ATTORNEY GENERAL

CONSUMER ALERT

Online Shopping Tips

KEEP YOUR DEVICES SECURE AND ONLY SHOP ON SECURE WEBSITES

Before you go online to shop, secure your computer or mobile device with up-to-date anti-virus and anti-spyware software. To make sure your devices have the latest protections, set your operating system and your web browser to update automatically.

Also, use a pop-up blocker and do not open files, click on links, or download programs sent to you unexpectedly or by strangers, since this is a common way to expose your device to a virus or malware.

If you are going to shop using a public wi-fi (not recommended), then before you send any personal information like your account or payment information, look for indicators that you are on a secure website, like a URL that begins with https (the "s" stands for secure) or a lock icon (🔒) in the browser window before the web address. Beware that unlike a secure wireless network that protects all of the information you send on the network, using an encrypted website protects only the information you send to and from that site.

- If you are going to shop while using a public wi-fi, consider installing a Virtual Private Network (VPN) that will allow you to securely send and receive information on a shared or public network as if you were using only a private network.

Finally, if you are shopping online using a mobile device: set up a remote wipe that allows you to take everything off your device if it is stolen; enable a find-your-device option so it can be found if you misplace your phone or if it is stolen; select settings to make your device undiscoverable; and turn Bluetooth off when you are not using it.

DO YOUR RESEARCH AND PAY ATTENTION TO DETAILS

To learn more about a product, brand or seller, type the name into a search engine with words like "review," "complaint" or "scam." You can also check out a company by contacting the Michigan Attorney General's Consumer Protection Team (mi.gov/agcomplaints) or by searching the Better Business Bureau's website (bbb.org).

Avoid online retailers if you cannot verify their listed physical locations and customer service phone numbers. Anyone can set up an online shop, list a physical location and phone number — that does not mean the business is legitimate. Research unfamiliar companies before you place an order.

- Do an online image search of the product and any other images the seller has posted to see where the product is coming from; how much it really costs; and who else is selling it. Watch this video to learn how to do that (youtu.be/VBHtZ3W7fmo).

The Better Business Bureau reports the most common place to find sites selling counterfeit goods is on social media, particularly Facebook and Instagram, which share the same ad network. A study by two cybersecurity experts found that one in four Facebook ads for fashion and luxury goods are linked to websites selling counterfeits.

The International Trademark Association has warned consumers about shopping on social media and encourages anyone shopping online to check a brand's list of authorized retailers and look for suspicious errors in spelling of the brand name or trademark. Researchers report difficulty distinguishing real from fake items based on Instagram images and even trademark holders of a brand have difficulty spotting a fake unless they actually buy the item. Read about more online shopping tips in the Attorney General's alert, "Drop-shipping: What You Need to Know Before You Buy or Sell Online."

And even if a product is not counterfeit, read the seller's description carefully — especially the fine print. Is it "refurbished," "vintage," "gently used" or a "close out"? A bargain price may mean the item is in less-than-new condition.

Pay attention to the terms of the deal. What is the delivery date? (Federal law requires sellers to ship items as promised or within 30 days after the order date if no specific date is promised.)

What is the refund policy? Can you return the item for a full refund? Who pays shipping costs? Are there any restocking fees?

Beware Tricks and Tactics Designed to Get You to Spend More

Have you ever bought something online because a notice popped up suggesting that the item was nearly sold out? Or perhaps you've bought something under pressure because a timer urged you to complete your purchase before your item is deleted from your cart? These common online selling tactics are called "dark patterns," and they are used by online retailers to play on shoppers' emotions, insecurities and biases when they shop online.

Experts warn that these ploys are not limited to online shopping sites, and that consumers should be suspicious on any website where it can benefit the online retailer to mislead you.

Don't get fooled, here's what to look for:

- Notices that a product is nearly sold-out.
- Timers that limit the time a product can stay in your shopping cart.
- Messages that suggest there is high demand for every item in your shopping cart.
- Countdown timers that restart when your refresh the webpage.

PROTECT YOUR PERSONAL INFORMATION

In addition to only shopping on a secure website, never use text or email to send your personal or financial information like your credit card, checking account, or Social Security Number — it is not secure. And try to give as little personal information as possible when you place an order. Some sites sell your information to other merchants, direct marketers, and even telemarketers.

Know where your personal information is going and know how the company will protect your personal and financial information. You should be able to learn both by reading the company's privacy policy. If you cannot find it, or you cannot understand it, consider ordering from a more user-friendly site.

Uncheck any box that allows the seller to share any of your information or that signs you up to receive more offers or communication from the seller other than updates about your order. (You can also do a control/find search for "opt out" language in any terms of agreement or posted privacy policies.)

Create an email account for use only when shopping online.

PAY WITH A CREDIT CARD

Under the Fair Credit Billing Act, a federal consumer protection law, your liability for unauthorized use of your credit card tops out at $50. However, if you report the loss before your credit card is used, you are not responsible for any charges you didn't authorize. If your credit card number is stolen, but not the card, you are not liable for unauthorized use.

Avoid using your debit card for online purchases because that gives criminals easier access to your checking account and it can be harder to fix problems.

Using a credit card will also protect you if you fall victim to a new online shopping scam called e-skimming. It happens when an online site is hacked, and malicious credential-stealing software is installed that allows criminals to steal your payment information from the shopping cart in real-time. You and the retailer may not be aware this happening. You check out with your payment information and your item arrives as you expected, but the hacker has your information and is using it or selling it to other scammers.

Additional precautions you can take include:

- Avoiding entering your credit card details into a website. Many online retailers will store your payment information in your account so you do not need to enter it into a web form where the skimmer may be lurking.
- Use a payment system like Apple Pay or PayPal, to skip entering your credit card information directly into an online site.
- Enable real-time alerts on your financial accounts to spot unauthorized activity.
- Review your accounts regularly so you can promptly dispute any charges you did not make.
- Consider using a low-limit card for online purchases.
- Access online stores by entering the web address yourself or a using a bookmark that you created. Avoid clicking on banner ads for a specific store or product, since those are likely to take you to a fake site or install malware.

Keep Your Receipts

Keeping your receipts will make a return easier, but it will also help protect you from "phishing" scams. Identity thieves send consumers emails from popular online merchants that look like a standard order confirmation email. To lure the consumer in, the email will include a fake order number in the subject line. Unsuspecting consumers who open the email may be at risk of downloading a virus or spyware. To avoid this scam, compare the real order number (from your saved receipt) to any "confirmation" or update emails from the merchant before you open them.

Report Fraud

To report fraud or if you have a general consumer complaint, contact the Michigan Attorney General:

1. Online: mi.gov/agcomplaints
2. Phone: 517-335-7599
3. Fax: 517-241-3771
4. Mail:
   Consumer Protection
   P.O. Box 30213
   Lansing, MI 48909