



Back-to-Learning Shopping is Here! Follow these 10 tips for safe online shopping

Since the pandemic, online shopping has increased dramatically. With schools starting out virtually for the new year, families will continue to buy from sites that offer fast delivery, great prices or curbside pick-ups. With the number of online transactions growing each year, thieves and fraudsters are eager to take advantage of our desire to buy online.

Here are 10 tips before you hit the “purchase” button to avoid falling victim to scams.

1. Use familiar web sites

It can be tempting to use a search engine to find great buys online; however, search results could show you sites that operate by overcharging, selling rip-offs, and/or failing to deliver products. To be safe, stick to well-known websites.

2. Use only secure websites

You should only share details like your credit card or banking information on websites with SSL (secure sockets layer) inscription installed. It's easy to see if a website has this added layer of protection—the URL will start with HTTPS:// (notice the “s” in there, for “secure”) and a locked padlock icon will appear in the window of your internet browser.

3. Don't share more info than needed

There is no reason a legitimate seller needs your social security number, birthday, mother's maiden name, etc. to verify your payment method. This is a red flag for potential fraud.

4. Wi-Fi

Even if you make sure to only use verified, secure websites for your online shopping, your information could still be compromised (i.e. stolen, logged, tracked) if you share it on an unknown Wi-Fi network/hotspot. If you do decide to use an unknown or free Wi-Fi, opt to use a gift card to make a purchase.

5. Malware

Protect your laptop or desktop against malware with an updated anti-virus program. By doing this, you'll also be protecting your financial information when you make purchases online.

6. Only use secure payment methods

Your Spidey senses should tingle if a website asks for you to pay with money orders, wire transfers, or checks. That's because these payment methods do not offer any buyer protection. Stick to credit cards or known online payment methods.

7. Check your credit card statements regularly

It's always a good idea to check your credit card statement after making an online purchase. Most transactions will show up on your online statement within 24 hours of making the purchase.

8. **Use strong passwords**

Strong passwords (at least seven characters long with upper- and lowercase letters, numbers, and symbols) that aren't used across multiple sites and are frequently changed will guard you against scammers guessing the password or a data breach. To keep track of your passwords, use an online password manager.

9. **Beware of fake mobile apps**



They do exist, and the trickiest ones will look very legitimate. Like malware, the aim of these apps is to steal your personal and financial information and compromise your identity. Be sure the app is shown on the company's website, check for ratings from other users, and avoid being the first to download an app.

10. **Too good to be true**

If it feels like a once-in-a-lifetime, too-good-to-be-true price for a usually expensive item, it probably is. Avoid clicking on pop-ups or visiting an unfamiliar website for that extra-special deal. It may just be a way for fraudsters to get the information they need.



This is an advertisement. Nymeo Federal Credit Union
Copyright 2020



[Unsubscribe](#)

Nymeo Federal Credit Union | 240-436-4000 | 855-436-4100 | nymeo.org
5210 Chairmans Court, Frederick MD 21703