



HOLIDAY SHOPPING TIPS AREN'T JUST FOR THE HOLIDAYS

1. Keep your computer and smart phone operating systems and software up to date.
2. Before you “click here” double-check that an email, social media, or an offer via text is legitimate. Especially if the text or email is unsolicited by you.
3. Research products by reading reviews on multiple sites. Don't rely on one site for reviews as it is hard to spot fake ones.
4. Make sure a website has an “s” after the http in the URL, as in *https*, the 's' means the website uses secure protocol and the website is safe. If you provide personal information on an unsecure site, it can lead to identity theft.
5. Remember, if the deal is too good to be true, it is too good to be true.
6. Use strong passwords and multi-factor authentication (MFA). While it is time consuming to set up MFA, undoing identity theft takes much longer.
7. Don't set up accounts on shopping sites, log in as a guest. Setting up an account provides scammers (and companies for that matter) more information about you than necessary. Keep your personal information to yourself.
8. Do not store your credit card on a company's website. If the company gets hacked, your information goes with it.
9. Never click on a social media advertisement to buy something. Go directly to the website.
10. If you have never heard of a company, but are tempted to buy something on that website, do an internet search with the name of the company plus scam, and see what comes up.



11. Verify that an email, text, or phone call claiming that there is an issue with your shipment, or purchase is a legitimate outreach. Scammers can create emails and texts to look like and pose as a real delivery service, such as FedEx, UPS, or the shopping site, such as Amazon. Call the company or go to the company's website directly before clicking on any email, or text.
12. Don't wait for your bill to come at the end of the month. Go online regularly to view electronic statements for your credit card, debit card, and checking accounts. Look for any fraudulent charges, even originating from payment sites like PayPal and Venmo.