

The Most Wonderful Time of the Year

Black Friday (Nov. 25) and Cyber Monday (Nov. 28) are almost here, the two busiest internet shopping days of the year used to kick-off the Holiday shopping season. Now, with sites offering pre-sales and early deals, some shopping has already started! So whether you start early, or wait until the last minute to shop, here are some tips to keep your internet shopping safe, merry, and bright.

- Stick to recognizable websites, and always verify the URL before entering any personal information. Check the website address (URL) to be sure it begins with "https:" instead of "http:" and for a padlock icon. If the padlock is closed, the information is encrypted.
- Avoid using a debit card for your purchases; use credit cards instead since there are limits to your liability for fraudulent charges should your card be lost or stolen.
- Avoid any deals that are too good to be true, especially free merchandise or gift cards. They're usually scams designed to steal your information.
- Beware of public Wi-Fi. It's not secure, so don't use it for sharing sensitive information while shopping.

Additional areas you will want to keep an eye on...

EMAIL

Watch for:

- Fraudulent "order confirmations" or "shipping alerts"
- E-cards that want you to open an attachment or click on a link
- Fake notices about your credit card being compromised
- Emails requesting information

What to do:

- Be suspicious of any unexpected email that wants you to click on a link or open an attachment, or asks you to confirm a purchase or account information.
- Hover your mouse over a link to see the real URL. If the two don't match, or the link seems strange, don't click!
- Beware of any offers you received by email or text from merchants you don't know. It could be a phishing attack.
- If you're even slightly in doubt, delete the email.
- If you're worried it might be real, contact the sender (your bank, FedEx, the store that is claiming to send the order confirmation) and see if you can verify the email's legitimacy.



SOCIAL MEDIA Scams:

- Pressure-driven "Black Friday" or "Cyber Monday" shopping scams
- Questionable charities
- Holiday-themed games, apps, or wallpapers that are infected with a virus

What to do:

- Use extra caution with anything related to "Black Friday" or "Cyber Monday." Stick with well-known stores and visit their sites directly instead of clicking on links.
- Only support charities you know are legitimate. Give directly on their websites.
- Don't download unknown software on your devices. Better to check out some known sites and read the reviews, than to fall for a flashy ad to download something that might turn out to be anything but festive

Now you're ready to go find that perfect toy for the kids, new electronic device for family, or something great for yourself on Cyber Monday - safely and securely. You got this!