ONLINE SHOPPING SAFETY DURING THE HOLIDAYS

Black Friday and Cyber Monday are like Christmas to cybercriminals, because they know that shoppers are looking for the best deals on high-ticket items. They'll be on the prowl for your login, card, and personal information.

There are some steps you can take to protect yourself and your information before you set out shopping. The first step is STOP. THINK. CONNECT.

- Go through a small but thorough cybersecurity checkup on all your devices: update all your programs and operating systems, check that your firewall is on and that your antivirus is up to date and running
- Avoid shopping on public or open networks
- Develop healthy password habits or use a password manager
- Check your account statements weekly through the end of the year; this will limit your risks
- Pay special attention to your store credit card statements when you shop this season, and consider getting the app to keep track; cybercriminals target these accounts because their security isn't as tight as with other cards
- Rather than shopping from email offers, consider using the known business sites from the sellers you know and trust; it's safer and helps forestall phishing scams
- Read through emails before clicking links: be on the lookout for typos or offers that seem too good to be true
- Hover over the links and verify the address without clicking them:
- Do you have a short link? Use a free tool like Short URL Check
- Want to check the link without opening it? Use a service like URLVoid to check
- Do you want to check on the sender's IP: try IPVoid, also free
- Make sure transactions are secure before clicking the purchase button: look for the 'https' sign of a secure connection.

This advisory is brought to you by OAS FCU.