SAFE Advisor

A quarterly publication from WESTprotect

Nov 2020

Holiday Scams - What to Watch for and How to Handle Them

As you navigate your way around the internet this season for shopping, posting on social media to family and friends, and enjoying the holidays, it's essential to be aware of potential online scams and have some actionable steps to follow should they intrude on your festivities. Here are some common ones to keep your eye out for - and what to do about them to stop them in their tracks!

Phishing emails are among the most common online threats, so it is important to be aware of the tell-tale signs and know what to do when you encounter them.

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 receive 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 think the message might be real, contact the sender (your bank, FedEx, the store claiming to send the order confirmation) and see if you can verify the email's legitimacy.

continued from previous page

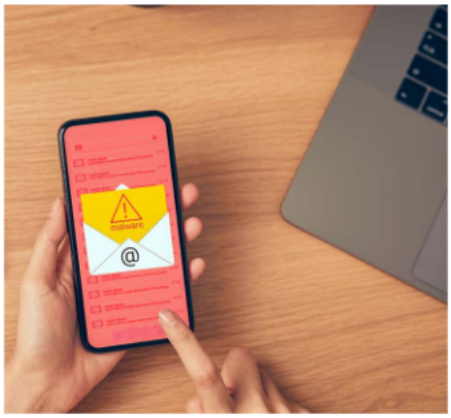
Social media is a great way to stay in touch with others, share thoughts, and follow topics that interest you. But it's also a way for others (bad guys) to catch your attention with timely offers, entertaining distractions, and requests for money.

Watch For:

- Pressure-driven " Black Friday" or "Cyber Monday" shopping scams
- Questionable charities
- Holiday-themed games, apps, or wallpapers that could be 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 personal devices, and check with your company's policies to see if you're allowed to download software on work devices.

To app, or not to app. Are you feeling lucky? Hundreds of fake retail and product apps can pop up in mobile App Stores at this time of year.

Watch For:

- Apps that request Facebook or credit card information – these can open you up to identity or financial fraud.
- Apps that could have malware to steal your personal information or lock your phone until you "pay a ransom."

What to do:

- Don't download any retail apps this year if you can avoid it. If you must, do your research before downloading.
- Beware of public Wi-Fi. It's NOT secure, so don't use it to conduct sensitive business, like banking or shopping. If you must use it, be sure to use a Virtual Private Network (VPN).

These tips should help relieve some of the worry and stress about scammers interfering in your holidays by knowing you have a plan should they try to scam you. Happy Holidays!

west protect

SAFE Advisor

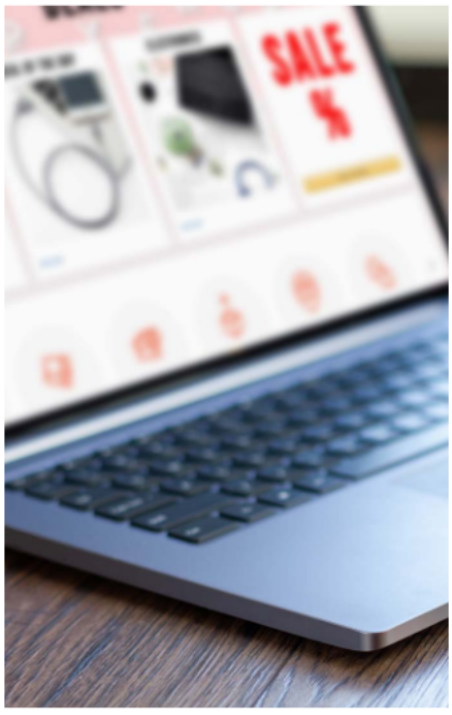
A quarterly publication from WESTprotect

Secure Holiday Shopping Online

We are less than a week away from Black Friday (27th) and Cyber Monday (30th), the two busiest internet shopping days of the year. This holiday season, even more shoppers will be ordering and purchasing gifts and services online and staying in touch with family and friends on social media and video conferencing. As this shopping season gets underway, we should be aware of potential holiday scams and malicious cyber campaigns, particularly when browsing or shopping online.

continued on next page

The FBI reminds shoppers that criminals don't take the holidays off and that thousands of people become victims of holiday scams every year. As usual, cybercriminals will be making the most of this year's opportunities to get between you and your money and try to steal your sensitive information - but don't despair. There are steps you can take to better secure your accounts, your transactions, your personal information, and keep your holidays happy and joyful.



Do you know where you're shopping?

Every year, fake e-commerce sites are spun up by fraudsters that look very real and can easily fool shoppers looking for that perfect gift at a great price. Once you go online to find the best deals - and before you start a purchase on a website you are not familiar with - check out the reviews to see what others have to say about it. See if there is an actual physical address or phone number you can contact to verify it's a legitimate business.

The best idea is to stick to recognizable websites and always verify the website address (URL) before entering any personal information. Check the URL to be sure it begins with "https" instead of "http" and a padlock icon. If the padlock is closed, the information is encrypted.

How much information is too much?

Before giving up any of your personal information, you should make sure the website you're shopping on has an online Privacy Policy and/or Terms of Use document, then read them carefully. If anything doesn't sound right or makes you uncomfortable about how they protect, use, or store your personal information - or worse, if they don't say - take your business elsewhere. Be aware of the types of information that are asking for you to provide. If you

continued from

SAFE:

feel they want more than they need, or if you're not comfortable giving the information they say is required, then don't! The cost of that particular purchase may not be worth it.

Debit card, credit card or third-party payment?

Using a credit card is much safer and better than using a debit card; there are more consumer protections for credit cards if something goes wrong with the sale. A debit card transaction is debited when the transaction occurs, so the money is immediately gone, and waiting to get your money back might leave you without the cash you may need for your other expenses. Better yet is the use of a third-party payment service. No matter which payment method you choose, be sure to monitor your credit card statements and bank account transactions to make sure there are no surprise charges. If you have the ability, you can also set up alerts for extra peace of mind that let you know whenever your cards are used.

Are you and your computer/mobile devices protected?

We've said this before, and we'll say it again because it's so important. Be sure to keep security software current on all devices that connect to the internet! Having the most up-to-date mobile security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.

Keep using strong passphrases or other features such as touch identification to lock your devices. Securing your devices can help protect your information if they are lost or stolen - and keep prying eyes out.

Be sure to use the available security and privacy settings on websites and apps you use to manage what is shared about you and who can see it.

Keeping things as secure as you can and following these suggestions will go a long way to a more stress-free holiday season for you and your family.