NOVEMBER 8, 2021 // MONDAY // ISSUE 3

# SECURITY NEWS

## HOLIDAY SHOPPING SAFETY


## Happy Thanksgiving!

**CHRIS MCDANIEL**
**NOVEMBER 2021**

The Yadkin County Information Technology Department would like to wish everyone a Happy and Safe Thanksgiving. It is finally that time of year again when we start planning our holiday shopping list before the big sales hit at the end of the month. We would like to remind everyone to stay security smart when shopping this year whether it be online or in store.

The newsletter I have put together this month will focus on Holiday Shopping Safety. Please take some time to read over the tips provided that will help keep you safe while shopping this year. Remember there are cybercriminals out there constantly looking for their holiday turkey to fall for their traps. Let's not fall prey to their tricks and always remember to think before you click.


## Online Holiday Shopping Scams

**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**
**NOVEMBER 24, 2020**

With more commerce occurring online this year, and with the holiday season upon us, the Cybersecurity and Infrastructure Security Agency (CISA) reminds shoppers to remain vigilant. Be especially cautious of fraudulent sites spoofing reputable businesses, unsolicited emails purporting to be from charities, and unencrypted financial transactions.

CISA encourages online holiday shoppers to review the following resources.

- CISA's Online Shopping Tip
- CISA's Holiday Online Shopping page
- CISA's Social Engineering and Phishing Attacks Tip
- The Federal Bureau of Investigation's (FBI's) 'Tis the Season for Holiday Online Shopping Scams - Don't Be a Victim Announcement

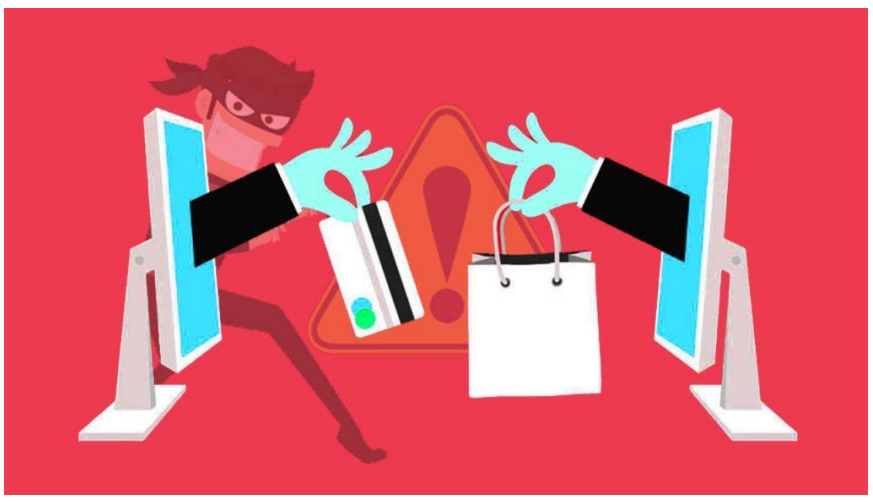
If you believe you are a victim of a scam, consider the following actions.

- Report the incident to your local police, and file online reports at the Federal Trade Commission's Report Fraud page and the FBI's Internet Crime Complaint Center (IC3) page.
- Watch for unexpected or unexplained charges to your account. If any appear, contact your financial institution immediately and close any accounts that may have been compromised. See CISA's Preventing and Responding to Identity Theft Tip for more information.
- Change any passwords you might have revealed immediately. Avoid reusing passwords. See CISA's Choosing and Protecting Passwords Tip for more information.

The information for this article provided by the Cybersecurity & Infrastructure Security Agency and may be found via the link provided here: Online Holiday Shopping Scams.

# *Shopping Online Securely*

**Mark Orlando, SANS, November 1, 2021**



## Overview

The holiday season is coming quick. Soon millions of people will be looking to buy the perfect gifts, and many of us will began shopping online. Unfortunately, cyber criminals will be active as well, creating fake shopping websites and other online shopping scams to steal your information or money. Learn how you can find good deals without becoming a victim.

## Fake Online Sites

Criminals create fake online stores that mimic the look of real sites or use the names of well-known stores or brands. When you search for the best online deals, you may find yourself at one of these fake sites. By purchasing from such websites, you can end up with counterfeit or stolen items, or your purchases might never be delivered. Take the following steps to protect yourself:

- When possible, purchase from online stores you already know, trust, and have done business with previously. Bookmark these online stores.
- Be suspicious of ads or promotions on search engines or social media that are significantly lower than those you see at the established online stores. If a deal sounds too good to be true, it may be a scam.
- Be careful with websites that have no way to contact them, broken contact forms, or use personal email addresses.
- Be suspicious if a website looks just like one you've used in the past, but the website domain name or the name of the store is different. For example, you may be used to shopping at Amazon, whose website address is www.amazon.com, but end up at a fake website that looks similar, but has the website address www.amazonshoppers.com.
- Type the name of the online store or its web address into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake."
- Protect your online accounts by using a unique, strong password for each of your accounts. Can't remember all your passwords? Consider storing them all in a password manager.

## Scammers on Legitimate Websites

Keep your guard up even when shopping at trusted websites. Online stores often offer products sold by third-parties - different individuals or companies - that might have fraudulent intentions. Such online destinations are like real-world markets, where some sellers are more trustworthy than others.

- Check each seller's reputation before placing the order by reading their reviews.
- Be wary of sellers who are new to the online store, lack reviews, or who sell items at unusually low prices.
- Review the online store's policy on purchases from such third parties.
- When in doubt, purchase items sold directly by the online store, not by the third-party sellers that participate in its online marketplace.
- Even with legitimate vendors, be sure that you understand the seller’s warranty and return policies before you make your purchase.

## Online Payments for Purchases

Regularly review your credit card statements to identify suspicious charges. If possible, enable the option to notify you by email, text, or app when a charge is made. If you find any suspicious activity, report it to your credit card company immediately. Use credit cards instead of debit cards for online payments. Debit cards take money directly from your bank account; if fraud is committed, you'll have a much harder time getting your money back. Electronic payment services or e-wallets such as PayPal are also a safer option for online purchases, since they do not require you to disclose a credit card number to the vendor. Avoid websites that only accept payment in cryptocurrency or require obscure payment methods.

Just because an online store has a professional look does not mean it's legitimate. If the website makes you uncomfortable, don't use it. Instead, head to a well-known site you can trust or have safely used in the past. You may not find that incredible deal, but you are much more likely to avoid getting scammed.

The information for this article from SANS may be found via the link provided here: SANS OUCH! Newsletter.

## ONLINE SHOPPING TIPS


NATIONAL CYBERSECURITY ALLIANCE

### TIPS FOR SAFE ONLINE SHOPPING

As more consumers purchase goods and services online, cyber criminals take advantage of this opportunity to swoop in and steal your sensitive information. There are steps consumers can take to better secure accounts and transactions.

#### TAKE-ACTION TIPS

**KEEP A CLEAN MACHINE**
Before making any online purchase, be sure that all internet-connected devices – including PCs, smartphones and tablets – are running only the most current versions of software and apps.

**USE A SECURE WI-FI**
Using public Wi-Fi to shop online while at your favorite coffee shop is tremendously convenient, but it is not necessarily cyber safe. Don't make purchases via public Wi-Fi; instead, use a Virtual Private Network (VPN) or your phone as a hotspot for a more secure shopping experience.

**LOCK DOWN YOUR LOGIN**
Create long and unique passphrases for all accounts and use multifactor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

**THINK BEFORE YOU CLICK**
If you receive an enticing offer via email or text, do not be so quick to click on the link. Instead, go directly to the company's website to verify the offer is legitimate.

#### GIVE AND TEACH

Purchasing an internet-connected device for a loved one? Don't assume they know how to use it securely. Take a moment to teach recipients how to configure privacy settings, how to deactivate any unnecessary features, and how to use the devices responsibly and securely. Don't let your loved ones learn the hard way. If you give them the gift, own your role in helping them understand how to use it securely.

the ame group

The AME Group is a Champion of National Cybersecurity Awareness Month, Privacy Day and STAYSAFEONLINE.ORG

staysafeonline

staysafeonline

KASPERSKY lab

### Tips for Safe Holiday Shopping

**1. Know who you are buying from**
Verify that the business is legitimate using sites like Epinions.com or BizRate.com.

**2. Be smart about your passwords**
Longer passwords reduce the chances of a hacker making a correct guess.
@4rg&*
grAf3FF

**3. Use secure sites for online transactions**
Mark sure the online stores you're shopping from start with https://.

**4. Use one credit card**
Dedicate one credit card for all your shopping needs.

**5. Beware of phishing attacks**
Don't enter sensitive or financial information into pop-up windows on suspicious emails.

**6. Update, update, update!**
Make sure your security software is up-to-date before shopping.
Update Anti-Virus Software

**7. Download secure apps only**
Use a mobile security solution so that you know the apps you download are safe.

**Did you know...**

- PASSWORD and 123456 are the 2 most commonly used passwords in the world
- Kaspersky Lab detects 125,000 new malicious programs every day
- 1400 new pieces of banking malware are created every day
- In August 2012, 290 brands were subject to phishing attacks
- $5.55 Billion Estimated total amount of credit card fraud worldwide

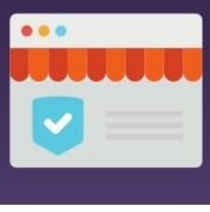
KASPERSKY lab

# SECURITY NEWS

DOs

**Buy from trusted sources.**

Use brands and shops that you are familiar with or have used before and check the ratings of individual sellers on sites such as Amazon or eBay.



**Control the recurring charges.**

Before providing your card details to pay for a continuous service over the internet, find out how you can stop that service.

Many e-merchant sites will ask to store your payment details.


**Think twice before deciding and make sure you understand the risks this might imply.**

**Use credit cards when purchasing things online.**


Most credit cards have a strong customer protection policy. If you don't get what you ordered, the card issuer will refund you.

**Make sure the data transfer is appropriately protected.**

Look for the padlock symbol on the URL bar and use HTPPS and SSL protocols when browsing over internet.

https

**Always save all documents related to your online purchases.**

They may be needed to establish the terms and conditions of the sale or to prove that you have paid for the goods.

# GOLDEN RULES

## SAFE ONLINE SHOPPING

EUROPOL EC3 European Cybercrime Centre

DON'Ts

**If you are not buying a specific product or service, don't submit your card details.**

**When purchasing something online from another person,**

don't send money upfront to the seller. If possible, reserve the right to receive the goods first.

**Don't send money to anyone you don't know.**

If someone approaches you online and asks for money, think whether you would give the same amount to an unknown person on the street.


**Never send your card number, PIN or any other card information to anyone by e-mail.**

**Avoid doing your online shopping at sites that don't use full authentication (Verified by Visa / MasterCard Secure Code).**


**Never send your card details in an unencrypted e-mail.**


Some online shops outside of Europe may request a copy of your card and passport by fax as a guarantee.