DCSA Cyber Awareness Message Cites Crucial Consumer Tips for the Holiday Season

QUANTICO, Va., Dec. 14, 2021 – As the holiday season is in full swing, the Defense Counterintelligence and Security Agency (DCSA) reminds its stakeholders who use computers and electronic devices – including more than 263 million consumers who shop online in the U.S. – to remain vigilant and increase their cybersecurity practices.

This cyber awareness reminder – like many issued by military commands and government agencies during the holiday season – is hoping to keep cyber incidents at bay through vigilance and security minded practices.

"As many increase their cyber footprint and online activities during the upcoming weeks, remember cyber threats do not take leave for the holidays," said Andrew Lochli, DCSA Threat Directorate assistant director. "Practice good cybersecurity hygiene and remain vigilant."

Bad actors taking advantage of consumers throughout the year are looking for more opportunities to commit cybercrime with fake websites, malicious links and fake charities throughout the holiday season. According to the National Institute for Standards and Technology, 2021 is already a record year for cyber vulnerabilities.

"While inter-connectedness and reliance on technology is an integral aspect of our everyday lifestyle, it also opens the door for cyber criminals, bad actors and adversaries – do not give them more opportunities," said Lochli in regards to various methods such as infected links and files within phishing messages that cyber criminals use to steal money as well as personal and financial information to commit identify theft.

Consumers can protect themselves online this holiday shopping season by taking a few easy steps to avoid becoming a victim of cyber-crime.

These steps to improve online safety include using strong passwords, updating software, thinking before clicking on suspicious links, and turning on multi-factor authentication.

- Implement multi-factor authentication on your accounts and make it 99% less likely you'll get hacked.
- Update your software. Turn on automatic updates.
- Think before you click. More than 90% of successful cyber-attacks start with a phishing email.
- Use strong passwords, and ideally a password manager to generate and store unique passwords.

This year's tips from the FBI to avoid holiday scams by practicing good cybersecurity hygiene – https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/holiday-scams – pertain to buyers and sellers.

- Don't click any suspicious links or attachments in emails, on websites, or on social media. Phishing scams and similar crimes get you to click on links and give up personal information like your name, password, and bank account number. In some cases, you may unknowingly download malware to your device.
- Be especially wary if a company asks you to update your password or account information. Look up the company's phone number on your own and call the company.

Know Who You're Buying From or Selling To

- Check each website's URL to make sure it's legitimate and secure. A site you're buying from should have https in the web address. If it doesn't, don't enter your information on that site.
- If you're purchasing from a company for the first time, do your research and check reviews.
- Verify the legitimacy of a buyer or seller before moving forward with a purchase. If you're using an online marketplace or auction website, check their feedback rating. Be wary of buyers and sellers with mostly unfavorable feedback ratings or no ratings at all.
- Avoid sellers who act as authorized dealers or factory representatives of popular items in countries where there would be no such deals.
- Be wary of sellers who post an auction or advertisement as if they reside in the U.S., then respond to questions by stating they are out of the country on business, family emergency, or similar reasons.
- Avoid buyers who request their purchase be shipped using a certain method to avoid customs or taxes inside another country.

Be Careful How You Pay

- Never wire money directly to a seller.
- Avoid paying for items with pre-paid gift cards. In these scams, a seller will ask you to send them a gift card number and PIN. Instead of using that gift card for your payment, the scammer will steal the funds, and you'll never receive your item.
- Use a credit card when shopping online and check your statement regularly. If you see a suspicious transaction, contact your credit card company to dispute the charge.

Monitor the Shipping Process

- Always get tracking numbers for items you buy online, so you can make sure they have been shipped and can follow the delivery process.
- Be suspect of any credit card purchases where the address of the cardholder does not match the shipping address when you are selling. Always receive the cardholder's authorization before shipping any products.

Remember that if a deal seems too good to be true, it probably is. This old proverb applies while shopping online during the holiday season or any time of year.

A few More Crucial Tips

- Buy only from trusted and established online retailers and avoid websites of retailers you've never heard of.
- Shop securely. While online, remember to check and protect your devices; shop through trusted sources via encrypted websites; and use safe methods for purchases. Check to make sure you're shopping on a site that uses SSL protection. The easiest way to tell is to check your browser's address bar. Look for "https" in the URL. Sites without the "s" are not safe to submit payment information or other personal details. Cybersecurity and Infrastructure Security Agency explains more about holiday shopping safety here: https://www.cisa.gov/sites/default/files/publications/Holiday%20Online%20Safety_tip%20sheets_2020-v5-DW_508%20pobs.pdf
- Use secure Wi-Fi. It's convenient but not cyber safe to use free public Wi-Fi to shop online. Use a virtual private network (VPN) or your phone as a hotspot.

- Take a moment to review your online financial accounts and ensure all transactions are your purchases. Take advantage of text and email alerting services offered by many banks and credit card companies.
- Resolve to have better cybersecurity in your social media life – check out this guide from Center for Development of Security Excellence: https://www.cdse.edu/Portals/124/Documents/jobaids/cyber/Twitter_Social_Networking_Site_Configuration_Guide.pdf?ver=1g4ckWrFs9HPGzkrm1V3zw%3d%3d