ALERT: Black Friday & Holiday Shopping Scams

U.S. Senator Maggie Hassan (D-NH), Ranking Member of the Joint Economic Committee, is leading a comprehensive investigation into the soaring rates of scams, which accounted for $1 trillion in losses globally last year and now surpass the drug trade as an illicit industry. Overall, Americans lose more money each year to scams than to burglary or car theft.

With Black Friday and the holiday season around the corner, Senator Hassan is working to raise awareness about common cyber shopping scams and provide Americans with practical tips.

The Holiday Shopping Season is Rife with Online Scams

Last year, the Thanksgiving holiday weekend drew around 124 million online shoppers and saw a record surge in online sales.

- Online shoppers spent $10.8 billion on Black Friday and $13.3 billion on Cyber Monday – the biggest-ever online shopping day.
- During the peak of online sales on Cyber Monday, consumers spent $15.8 million *every minute*.
- More than 69 percent of all purchases on Black Friday were made using mobile devices.

Scam activity also skyrocketed during this time.

- Black Friday scam websites, most of which impersonate top brands to steal a victim's personal information or dupe them into paying for nonexistent or counterfeit merchandise, surged by 89 percent last year, compared to the year before.
- Criminals lure victims to these sites through targeted social media ads, sponsored search results, and phishing campaigns. In 2024, three out of four Black Friday spam emails were outright scams, while the remainder were just "overly aggressive promotions," according to a cybersecurity firm.
- Phishing emails that mimic major U.S. retail brands, including Walmart, Target, and Best Buy, increased by more than 2,000 percent during peak holiday shopping periods last year.
- Black Friday and Cyber Monday phishing scams increased by almost 700 percent between early November and the busy shopping days.

With online holiday sales expected to increase again this year, consumers need to stay informed and remain vigilant.

Below are some practical ways to spot and protect yourself from common online shopping scams, including tips from the FBI, Better Business Bureau (BBB), and Federal Deposit Insurance Corporation (FDIC).

Tips for Combating Common Online Shopping Scams

- Be skeptical of deeply discounted items. If a deal seems too good to be true, it often is.
- Look out for suspicious emails, phone calls, and texts, including messages from unknown numbers or from email addresses that do not match official company websites.
- Be wary of emails that demand urgent action, such as resetting your password, resolving an issue with a package delivery, or claiming a bargain or giveaway that is about to expire – as scammers frequently try to rush their targets into providing sensitive information or making a fraudulent payment.
- Avoid clicking on links or downloading attachments from emails, texts, and social media, which can direct you to a fraudulent website or install malware on your device.
    - Instead, to address concerns with your account or verify a discount from a company you trust, go directly to the vendor's website. Do not use contact information listed in an email, text, or ad, which can steer you to a scammer.
- Research unfamiliar sellers on sites like BBB.org, where you can check customer reviews and complaints.
- Before making a purchase, look for signs of a fraudulent website, including misspellings, extra words, or unusual domains in the website's URL with extra characters or different spellings of popular brand names, for example.
- Ensure that any website where you are entering your payment information has "https" in its URL, which indicates that the site has a protected network connection.
- Use a strong password and enable two-factor authentication on your accounts, as this can make it harder for bad actors to access them.
- Monitor your bank account and credit card statements for suspicious transactions.
- Be wary of sellers who ask you to pay with a money transfer, cryptocurrency, or pre-paid gift cards. These irreversible, difficult to trace payment methods are a favorite of scammers.

For Victims

If you think you have been the victim of a scam, please visit ReportFraud.ftc.gov. If you reside in New Hampshire, you can also contact the New Hampshire Department of Justice Consumer Protection Hotline at 1-888-468-4454 or (603) 271-3641.

Please also consider sharing how you or your loved ones have been impacted by scams by completing Senator Hassan's online scams SURVEY. *This survey is informing Senator Hassan's ongoing investigation into scams and is not intended for individuals requesting assistance with fraudulent activity or seeking to file a report with law enforcement.*