

All About...

6 Shopping Scams and How to Avoid Them This Holiday Season

Spooky season just ended, so you can finally feel good about buying the Halloween candy that had been on the shelves since the day after Independence Day! It ALSO means the biggest online shopping day of the YEAR is just weeks away: Cyber Monday. Unfortunately, it's also open season for cybercriminals. Now that's *scary*. Because preparation is the best prevention, we're covering the six most common shopping scams this time of year and how to avoid them.

It's Open Season for Shopping Scams

Thanks to cybercriminals, what should be a season of festive shopping is now dangerous for consumers. According to the Federal Trade Commission, shopping scams were the second-worst type of scam in the US in 2023. And online scams are at their worst during the holidays. According to TransUnion's 2022 Global Digital Fraud Trends report, there was a 127% increase in daily fraud attempts between November 24 and 28 compared to January 1 through November 23.

Due to the high volume of shopping activity during the holiday season, cybercriminals don't have to work hard to find potential victims. But it's not simply volume that contributes to the rise in attacks; consumers take more risks during the holiday season. According to Norton's 2022 Cyber Safety Insights Report, nearly one in three adults (32%) worldwide admitted to taking more risks with online shopping closer to the holidays. Last-minute shopping pressure or excitement around scoring big deals results in common mistakes, including clicking on unverified links, using public Wi-Fi for transactions and ignoring website security red flags.

Cybercriminals expect shoppers to make mistakes, and they have tried-and-true tactics for stealing your money. Watch out for these six scams that appear this time of year and protect yourself this holiday season.

6 Common Scams During Black Friday & Cyber Monday and How to Avoid Them

1. Fake Coupons: Scammers distribute fake coupons promising steep discounts. These coupons are often shared via e-mail, social media and fake websites designed to mimic legitimate retailers. *If it feels too good to be true, it probably is!*

How to avoid: Always verify a coupon by checking the retailer's official website or app--and avoid clicking on links in unsolicited e-mails.

2. Phony Websites: To steal personal information, fake websites mimic legitimate online stores using similar logos, branding and URLs that are only slightly different from the official sites.

How to avoid: Check for secure website indicators such as HTTPS and a padlock icon in the address bar. Read reviews and quickly search the website's legitimacy before making any purchases. Pay attention to the URL for any unusual characters or misspellings.

3. Fake Delivery and Non-Delivery Scams: Scammers send fake delivery notifications or claim a package is undeliverable to trick you into providing personal information.

How to avoid: Track orders directly through the retailer's website or app. Avoid clicking on links in suspicious messages and be cautious of unsolicited delivery notifications.

4. Fake "Order Issue" Scams: E-mails claiming a problem with your order and asking for personal details are common. These messages often look like they come from well-known retailers.

How to avoid: Contact customer service directly through the retailer's official channels to verify any issues and avoid providing personal details through links in unsolicited messages.

5. Account Verification Scams: Scammers send e-mails or texts asking you to verify your account information. These messages often include links to fake login pages.

How to avoid: Never provide personal details through links in unsolicited messages; instead, log in directly to your account through the official website.

6. Gift Card Scams: Scammers offer discounted gift cards or request payment via gift cards. Once the card numbers are provided, the scammer uses the balance, leaving the victim with a worthless card.

How to avoid: Purchase gift cards directly from reputable retailers and never use them as a form of payment to unknown individuals.

Avoid Scams and Create a Safer Shopping Experience

Nothing will kill the holiday shopping spirit like \$1,000 worth of fraudulent charges on your credit card or gifts from phony sites that never arrive. Cybercriminals take advantage of the festive shopping rush, and consumers' tendency to take more risks during this time only amplifies the danger. By verifying sources, checking website security and avoiding unsolicited links, you can enjoy a safer shopping experience this season!

AND... if you're concerned about *your business's overall security*, don't wait for a problem to occur. **Schedule a FREE Security Risk Assessment with our team today**, and let's ensure your entire network is protected from top to bottom. Our experts will identify vulnerabilities and recommend tailored solutions to keep your business safe.

To get started, give us a call at 215-769-9980 or [click here](#) to book now.