6 Black Friday scams + how to avoid them in 2022

Written by Clare Stouffer, a NortonLifeLock employee October 18, 2022

The holiday season is right around the corner. Not only is this a wonderful time for seeing family and friends, but it's also a great time for savings, specifically on Black Friday. Black Friday draws millions of holiday shoppers seeking to score deals, compete for hot products, and cross names off their shopping lists.

In 2021, American shoppers spent **nearly $9 billion** on Black Friday alone. This flurry of shopping activity also attracts scammers looking to cash in. In fact, **one in four** shoppers reports experiencing fraud during the holiday season. Scammers can easily take advantage of the season to make off with your gifts, credit card information, or identity.

To ensure you can shop confidently and make the most of all the great holiday deals, we've gathered six common Black Friday scams to be aware of in 2022. Before you reach into your wallet this holiday season, follow this guide to learn more about Black Friday scams, protection tips, and what to do if you come across one.

1. Non-delivery scam

You're searching online when you come across the perfect gift at a good price. You go to the site, put the item in your cart, and click "Buy." You don't get a tracking number, the package never arrives, and the seller disappears. You're experiencing what the FBI calls a non-delivery scam.

You can avoid this by sticking to reputable retailers. If you're shopping with a new-to-you merchant, do your due diligence. Check for a physical address, a customer service phone number, and a professional-looking site. Warning signs of malicious websites include poor spelling, odd design, and slow loading times. Only buy from secure sites with SSL encryption — look for URLs starting with HTTPS (the "S" is important, rather than just HTTP) and a lock icon in the corner.

- **What to do if you fall for a non-delivery scam**: Document your unsuccessful attempts to contact the seller, collect screenshots or other proof of the problems, and ask your credit card company to reverse the charges due to fraud. If you paid with PayPal, an alternative is to **open a PayPal dispute**. Consider asking your credit card issuer to deactivate your old card and issue you a new one.

2. Gift card scam

You plan to use your favorite credit card to make your Black Friday or Cyber Monday purchases, but a seller asks you to pay with a gift card. This may happen on auction sites and should raise big red flags. Gift cards are often utilized by cybercriminals because it is an easy way for them to steal money from you.

Instead, stick to using a credit card for your online holiday shopping. By federal law, your liability for fraudulent credit card purchases is **capped at $50,** and virtually all card issuers offer $0 liability. Treat gift cards like cash, never giving out your gift card number or PIN, and using them only with the issuing merchant. For example, you'd use an IKEA gift card at an IKEA store or IKEA.com. Use general gift cards, such as a Mastercard or Visa gift card, only at a trusted retailer.

- **What to do if you fall for a gift card scam**: Contact the gift card issuer immediately to let them know your gift card was used in a scam. If you act quickly, they may refund you any money left on the gift card. Each major retailer has their own way to **report gift card scams**.

3. Fake charity scam

Scammers may take advantage of the holiday spirit by using heartwarming stories to get donations for **fake charities**. These Black Friday scammers know that charitable donations as holiday gifts have become especially popular in recent years.

To avoid this, never make an impulse donation in response to an ad or plea on social media. Take time to research charities using resources that track and rate nonprofits.

- **What to do if you fall for a fake charity scam**: If you've been scammed by a fake charity, report the scam. The FBI recommends contacting your state consumer protection division, The **FBI's Internet Crime Complaint Center (IC3)**, and the **Federal Trade Commission.** You probably won't get your money back, but you may help law enforcement catch the scammer.

4. Fake order scam

Criminals may use Black Friday shopping to put a holiday twist on **phishing** scams. In these Black Friday phishing scams, you may get an email or other message telling you there's an issue with an item you ordered, but you don't recognize the item and know you never ordered it. The message may be a phishing email meant to trick you into clicking a suspect link, providing your bank login credentials, or turning over other personal information to the criminal.

If you get a message about an item you didn't order, stop, and think. The criminal is trying to throw you off balance, hoping you'll take the requested action because you want to get to the bottom of the situation. If you're unsure if a message is legitimate, contact the business through other channels that you find on your own, such as an online chat or their customer service phone number.

- **What to do if you fall for a fake order scam**: If you do click on a phishing link, act right away. If you provided login credentials for any site, immediately change your username and password. With your Norton Password Manager, you can easily create secure, unique passwords and safely store them for your online accounts. If necessary, change your PIN number to help protect your banking information. Finally, report the scam to the authorities, including any legitimate business the scammers were impersonating, as well as the FBI's **IC3**.

5. Fake website scam

In another 2022 holiday shopping scam, you think you're going to the website of your favorite department store to score some Black Friday deals, but you accidentally misspell the name when typing it into your browser bar. You think you're on the real site, and you make a "purchase." The scammer uses this spoofed website to advertise fake Black Friday deals, steal your credit card information to use or sell, and possibly grab other personal information such as your name and address.

The easiest way to avoid a cloned site is to make sure you're going to the real site when you want to shop. And never visit a retailer by clicking a link in a "deal" email or on social media.

- **What to do if you fall for a fake website scam**: Immediately change your username and password for the real shopping site since the scammers likely got your login information. If

you've saved your credit card information on the real site, delete it as a precaution. If you used a credit card to make a purchase on the sham site, report the fraud to your card issuer. They will block the scammer from using your old card number and will issue you a new card with a new number and expiration date. For added protection when browsing online use Norton Safe Search, included in your protection plan, which helps you stay safe and avoid fake websites.

6. Fake delivery scam

With many consumers doing their holiday shopping online, cybercriminals are taking advantage of this by sending false delivery notifications via email or text message. These notifications may look like they're coming from the U.S. Postal Service, FedEx, or UPS. The scammers are betting you recently bought something online, and Black Friday and Cyber Monday improve their odds. They may mention a problem with delivery and provide a link you can click to "fix the problem." You may be asked to enter personal information or a credit card number.

Just knowing about this Black Friday scam is a good start. If you ever get an email or text about a delivery problem, don't click any links or call any number provided. If you think it may be a legitimate message, look up the company information on your own and contact them directly. If the message was not legitimate, let them know about the scam.

- **What to do if you fall for a fake delivery scam**: What to do in this scenario depends on what information, if any, you provided to the scammer. In general, it's a good idea to follow the same steps you would for a fake order scam (change your username and password and report the scam to the authorities), which is also a phishing scam. You may also want to keep a close eye on your accounts and consider monitoring for identity theft.

The hustle and bustle of the holidays is a gift to cybercriminals. That's why it's so important to know how 2022 Black Friday scams work and to take steps to help keep you, your family, and your property safe this season. And remember, you should always take steps to protect yourself from online shopping scams, even after the holiday season is over. Happy shopping!