

# Black Friday and Cyber Monday – Scams to look out for

Yes, it's that time of the year again with just 45 days to go before Christmas.

For retailers this is the best time of the year, and also the most profitable time for scammers. What I am talking about is Black Friday and Cyber Monday. This is something we should be aware of, regardless of where we live, as the internet respects national boundaries.

## Different between the two

Black Friday dates back to the early 1950s, when retail stores would kick off the Christmas shopping season with big sales. So big, in fact, that annual store profits would often tip into "the black" (meaning no longer "in the red," which was accounting parlance for losing money) once all the receipts were tallied.

Shoppers came in droves because the day after Thanksgiving was typically a day off, making it the perfect day to shop. In *stores*. Then the Internet happened.

This year, Black Friday is on 24<sup>th</sup> November and Cyber Monday on the 27 but deals can be found sooner than that.

## When did Cyber Monday start?

It's hard to believe, but Cyber Monday dates back to just 2005. Back then, before it was natural to order anything and everything online, shoppers still needed encouragement. Online stores began running their own big sales to compete with the brick-and-mortar juggernaut that was Black Friday.

Why "Cyber Monday"? Because in the old days, the internet was often referred to as "cyberspace."

Apart from the days, there are a couple of other differences between the two, one is that Cyber Monday applies only to online shops while Black Friday is in stores as well.

Also, Cyber Monday is a strictly 24-hour shopping window but Black Friday tends now to be a five day long affair.

## Scams to Avoid

From phishing sites to fake coupons, here are the Cyber Monday scams to avoid — and tips for shopping safer and smarter.

Cyber Monday is a day for deal-chasing. Deals will pop up and disappear quickly. Emails will land in your inbox, urging you to buy before it's too late.

Keep these safety tips in mind while shopping online this Cyber Monday.

### 1. Use credit, not debit

Maybe you use a debit card to avoid interest charges and prevent yourself from spending more than you should. But credit is far more secure than debit. If a thief steals your debit card info, you're far more vulnerable.

Most major banks will refund you completely for fraudulent debit purchases, but, in the meantime, you're out the money stolen (money you may need to pay your bills). Your credit card, however, is not linked directly to your bank account. A thief making a fraudulent credit card transaction has effectively stolen the bank's money, not yours.

Plus, credit cards provide extra purchase protections that debit cards don't, including [price protection](#) and [extended warranty coverage](#).

## **2. Be careful when clicking through to a retailer from emails**

You see an exciting deal from a retailer you frequently shop at pop up in your inbox and immediately click through. But did you double-check the URL the email sent you to?

"Most people will probably shop on sites they trust, but if you're using a new site or clicking through a link to a deal you received in an email, you may end up on a phishing site. "These sites are designed to steal your personal information and perhaps your payment information by posing as legitimate websites."

It's therefore vital to scrutinize every site you shop with. Is it really the site you think it is? One easy way to make sure a site is legitimate is to look at the URL bar and make sure the address matches the retailer's real URL exactly. Scammers are skilled at using misspellings or added paths in their URLs. Also check for "HTTPS," to ensure your data can't be intercepted.

Phishing emails are a big problem on Cyber Monday because shoppers are under more pressure to buy than usual.

### **Use a password manager**

Many merchants save your payment information to make it easier for you to buy more things in the future. And that makes having strong passwords (unique to each site) extra important.

"If your passwords are recycled or easy to guess, then an attacker could easily take control of your accounts and shop as if they were you,

So, if you are shopping on lots of new sites during Cyber Monday and recycling passwords for your accounts, you're setting yourself up for potential future theft.

A password manager ([see a roundup of the best ones](#)) will let you generate long, random passwords that are unique to every site you have an account with. It will then hold those passwords securely and auto-fill them anytime you return to those sites, so there's no need to create a simple, hackable universal password.

## **4. Watch out for fake coupons**

Fake coupons tend to pop up on social media during major shopping holidays.

Coupon scams generally start with a legitimate-looking image of a coupon with the retailer's logo in your feed and instructions to click the post to claim it. In reality, these coupons are cleverly designed phishing scams.

If the coupon post sends you to a survey, routes you to a site that asks you for personal information, or prompts you to download an app, you're definitely dealing with a coupon hoax. Another clue is a too-good-to-be-true offer. Even if the post seems to send you to the retailer's site, follow the advice above and double-check that URL.

Instead of chasing coupons in your social media feed, go to your favourite retailer's site directly, sign up for its email list or [check out current offers for your favourite retailers on our site](#).

### **5. Consider using mobile wallets for physical purchases**

If you're planning to make in-store purchases on Black Friday in addition to shopping online Cyber Monday, consider using a mobile payment app like Apple Pay, Google Pay or Samsung Pay rather than a physical card, suggests Neil Rubenking, lead analyst for security at PCMag.

Mobile wallets use a single-use token system that encrypts your card information. So, even if the retailer gets hacked, the information the data thieves steal won't be your real card number.

"It's more secure than the card, and it finishes much faster than a chip-card transaction," Rubenking says.

**David Thomas**

**President**

**Safe Communities Portugal 15<sup>th</sup> November 2018**