Top Tips for Safer Online Shopping on BLACK FRIDAY AND CYBER MONDAY

Black Friday and Cyber Monday have become established as two of the year's biggest shopping events, giving consumers the opportunity to snap up a stash of stunning bargains. While this is generally good news, of course, the resultant retail frenzy can lead to people dropping their guard – especially online. In previous years, a seasonal surge in cyber-crime has seen schemes such as phishing emails and credit card scams being unleashed on unwary buyers. Our guide has some essential pointers on keeping your details – and your money – safe while you shop.

ENSURE A SITE'S SECURE

Before inputting sensitive information (like your card details) into a website, check that the site's secure. The key thing is to look for a padlock symbol in the address bar and check that the URL begins with "https://" – the "s" indicates that the web address has been encrypted with an SSL certificate. Without that, any data entered on the site could be intercepted by criminal third parties.

TRUST YOUR INSTINCTS

If a deal seems too good to be true, then it probably is. Be especially wary if a site offering unbelievable discounts doesn't look professional (for example, if it's covered with pop-up adverts or it looks particularly outdated) – this often serves as a red flag that the seller might not be entirely trustworthy. Minimise risk by sticking with well-known, reputable retailers instead.

REVIEW BANK STATEMENTS

Even if you've followed all our tips, it's probably worth checking your next bank statement for any unusual transactions. Criminals know that on Black Friday and Cyber Monday, lots of people make numerous purchases online: they're hoping that any stolen money will get lost in the crowd of other transactions. If you see a payment or payee you can't identify, raise it with your bank straight away.

BEWARE OF SUSPICIOUS EMAILS

Black Friday and Cyber Monday often bring a significant spike in phishing emails, as criminals use the events' sense of urgency as cover for stealing personal information. Even if they look legitimate, be wary of emails requiring you to do something unusual or suspicious: providing your personal details in exchange for access to last-minute deals, for example, or clicking on a link to an unfamiliar site.

CHECK IT'S THE REAL DEAL

It's not just cybercriminals you need to be wary of. Research has shown that some online retailers increase the price of certain items in the weeks before Black Friday and Cyber Monday – enabling them to then advertise "discounts" (which, in reality, have simply restored the cost to normal levels). Use an online price comparison tool to verify whether these "reductions" truly equate to a saving.

MINIMISE MICROTRANSACTIONS

Black Friday and Cyber Monday promotions extend to digital items as well as physical ones. Some gaming companies will offer discounts on in-app and in-game microtransactions such as loot boxes. If you're concerned about how much your child might spend on these upgrades, you can restrict their ability to make purchases (via their device's settings) or remove any linked payment methods.

SET STURDY PASSWORDS

A strong, unique password is one of the most straightforward ways to protect yourself from cyber-crime. As most of us have multiple online shopping accounts, it can be tempting to use the same password for them all – but this puts your personal data at greater risk. You could try using a password manager to create a different, robust password for each online retailer that you visit.

DITCH THE DEBIT CARD

Where possible, it's safest to shop online with a credit card (as opposed to a debit card) because it offers additional protection. If a purchase is made fraudulently on your credit card, there's a fair chance of your bank reimbursing you. Should criminals obtain your debit card details, however, they could empty your account in moments – and it can be difficult to recover your money.

RESIST THE INFLUENCE

Recommendations from social media influencers are another thing to remain vigilant for on Black Friday and Cyber Monday. While many of these will be legitimate, remember that influencers are often paid to promote products – and to publicise deals that aren't quite as amazing as they might seem. Don't feel pressured into buying purely on their advice; look at everything with a critical eye.

TAKE CARE ON SOCIAL MEDIA

Social media scammers are more active on Black Friday and Cyber Monday, as they know people are hunting for deals online. These scammers tend to concentrate on platforms such as Facebook and Instagram, posting malicious links that can compromise shoppers' personal details. Other scammers, meanwhile, falsely advertise products in an attempt to trick users out of their hard-earned cash.

Meet Our Expert

Carly Page is an experienced technology journalist with a track record of more than 15 years in the industry. Previously the editor of tech tabloid The Inquirer, Carly is now a freelance technology journalist, editor and consultant.

National Online Safety®

#WakeUpWednesday