Black Friday and Cyber Monday shopping scams

Although there are some fantastic bargains to be made on what is known as Black Friday (this year 24th November) and Cyber Monday 27th November, unfortunately there are criminals who take advantage of this through various scams and on-line fraud**.**

According to a report from PricewaterhouseCoopers (PwC) 51% of UK shoppers plan to shop over Black Friday and Cyber Monday and three quarters of all spending will be done online or by mobile**.**

Black Friday 2017 itself is expected to be the biggest day of spending the country has ever seen with UK shoppers expected to buy £10.1bn worth of goods over the next week.

In Portugal on-line shopping fraud is the largest in terms of all on-line frauds and is increasing considerably.

To reduce the risk of becoming a victims here are some tips to follow.

Buy from traders you know and trust

When it comes to shopping online, it's always safest to stick to familiar shops and brands that you know you can trust.

There are some stores online that aren't mainstream brands but are still trustworthy places to shop. If you feel you must shop with an unknown trader, make sure you research them first. Usually the best thing to do is look for reviews of the website and a reliable way to contact the site owner that isn't just email in the event your delivery goes wrong.

The most obvious things to look out for that signal a scam website are, firstly, website quality and copy/editorial quality. Someone trying to make a quick buck out of you isn't going to labour over their website's UI and crafting flawless copy so if something about a website's design feels less than professional or you spot more than one spelling error it's worth being suspicious.

If you're not sure of a website, make sure you have a look at the URL when you're paying for your purchase. Any transaction you make should be on a page with an HTTPS link rather than an HTTP link as this ensures the transaction is safely encoded.

Deals too good to be true might be a sign of a scam. Read the fine print on who is behind the bargain, total price including delivery, policies on cancellation and refunds, and warranty terms.

Don't assume all is good if you see no complaints.

Often, scam artists set up shop just as quickly as they close down their fraudulent operations and make off with their loot. Don't be sold solely on the fact that a company or individual seller has no complaints. Do your homework and research unfamiliar vendors before offering up your personal info and credit card number. Those who don't are more likely to fall victim to Black Friday and Cyber Monday scams**.**

Don’t shop from a free Wi-Fi connection.

Protect your personal information when shopping online. The more private your Wi-Fi connection, the more secure your shopping transaction. Avoid coffee shops, airports, libraries, and anywhere that offers free (and vulnerable) connectivity without a password for online shopping. The same goes for online banking**.**

Pay securely

No matter where you’re shopping, always use a secure form of payment. This means opt for a credit card, a debit card, or even PayPal over any direct money transfers.

Credit card is probably the most secure option in terms of shopper rights as you can dispute charges made if your item never arrives or dispute any suspicious charges generally.

It's also a good idea to use two-factor authentication on your online shopping accounts wherever possible. It's not every retailer that has these, but it's worth noting that Amazon does. Two-step authentication simply adds another layer of security to your account, requiring you to enter a security code sent via text or call as well as your password when you're signing in.

Don't click on strange links

It doesn’t matter whether you’re on your laptop or on your phone or whether the link appears in your email inbox, WhatsApp messages or pops up on your Facebook News Feed, don’t click any strange or unfamiliar ad links.

It seems obvious but you don’t know where that link is going to go and what kind of malware is lying in wait there. There are few modern embarrassments quite like clicking one of those links that posts its deal from your account to every one of your Facebook friends or WhatsApp contacts; malware spreaders never get to take care of their friends’ cats.

Update your antivirus software

Speaking of which, accidents do happen so to avoid the worst make sure your antivirus and phone software is up to date so that you don’t fall victim to anything truly terrible.

Check returns policies

One thing that’s worth noting even with retailers you trust: check their returns policies. You may have managed to grab some great bargains but there’s no guarantee you’re going to be happy with all of them on delivery day. And we've all experience the impulse buy hangover.

Though return periods are usually extended during the holiday season, some retailers might not take part in this and some could have shorter return windows specifically for electronics, so it’s worth being aware of how long you have to make up your mind. If you do decide to return something make sure you know exactly what you need for proof of purchase as well as how and where you need to return it.

For sale items you might find a return is entirely out of the question, leaving you lumped with a gift card. Bearing this in mind, it’s worth checking whether this is the case before you commit to a purchase you’re not entirely certain of.

Since Black Friday is not the only time in the festive period prices will be cut, it's worth seeking out retailers that offer price promises so that if the item you purchased drops in price in the weeks following Black Friday you can be assured of a refund.

Lastly- Keep track of your spending.

Identity thieves bank on the fact that shoppers get caught in the holiday frenzy and pay little mind to whom and for what they've paid. Record your purchase details (order confirmation numbers, date and time of purchase, etc.) and regularly eagle-eye your banking and credit card statements. Then, be on the lookout for purchases, especially small ones, you might not have made. Often, crooks won't immediately go big in the hope of going unnoticed.