Grab the bargains on Black Friday… but be alert for potential cyber fraud

Submitted by: The PR Room
Thursday, 15 November 2018

London, 15th November 2018: Black Friday sales are a great opportunity to bag a bargain, particularly online. But while there are many Black Friday bargains to be had, cyber fraudsters also view this calendar event day as an opportunity for fraud.

More than 17 million Brits were hit by cybercrime in 2017. That said, there is no reason to avoid shopping online out of paranoia. Most stores and sellers are operated by legitimate businesses, however you should never become so comfortable with shopping online that you compromise your security through complacency.

Stay alert, observe safe shopping practices, and you will be able to enjoy the convenience and speed of Black Friday online sales without sacrificing safety. Cybersecurity company, BullGuard (http://www.bullguard.com/), has put together some useful tips that will help shoppers stay safe and avoid cyber criminals during the Black Friday sales.

Be alert for phishing mails
As Black Friday approaches cyber fraudsters get seriously busy crafting phishing emails. These emails are endlessly creative and claim to be from all sorts of organisations that you will know from well-known retailers, sports suppliers and even travel companies. The one thing they have in common is an offer that is too good to ignore. Except that's exactly what you should do, ignore and delete them. The aim of the fraudsters is to get you to click on a link. If you do and go on to enter personal information to the website page you clicked through to, you will have just handed your information over to a fraudster.

Shop on websites that you trust
Well-known brands have a track record of trustworthiness. Whenever possible, buy from vendors you trust on sites that you trust. That doesn't mean you shouldn't try out a new site or store, but if you have the option to shop somewhere safe and familiar for the same prices, it's a good idea to take it. It certainly makes life easier and removes uncertainty from the equation.

Check website security
It should be a golden rule that you avoid buying something from a website that doesn't have 'https' at the start of the URL. The 's' stands for secure and signifies encrypted data. You should also look for a green padlock in the browser bar as this also symbolises the same thing. If either of these things is missing, give the site a wide berth.

Poorly designed websites
If a website isn't professionally designed, it might mean that the owner of the site isn't a professional and could also be a scammer. Even if the vendor is well intentioned, the site could be compromised if the site design isn't competent.

A well-designed website is usually a good sign when you're shopping somewhere new. If you get a lot of pop-ups and cannot close them, it is best to stay away. Another red flag is when you navigate to a site

that is difficult or impossible to navigate away from. It’s a good warning sign.

Beware of social media scams

Your email account isn’t the only place you can receive phishing messages. Customers are often targeted on social media sites like Facebook, Twitter and LinkedIn. Scammers will often send a message that looks like it comes from the social media service itself, but the links in the message will take you to fake pages. Social media sites will never ask you for your user name and password in order to verify your account through a private message. Be very alert when you receive messages from unknown senders.

Be careful shopping online with mobile devices

When using a mobile device you can receive an abbreviated URL for a website. This can mislead buyers into phishing scams. For example, it is common to shorten URLs for display on sites like Twitter or even some shopping websites. However, since the URL is shortened it is impossible to know where you are being sent when you click the link.

You may also be tempted to shop on a public network, but these unsecured networks have security vulnerabilities. When using a mobile device make sure you are using a password protected network. On iPhones, secure networks will have a little padlock next to the network name when you connect. Other operating systems will have a similar technique for showing secure networks that you should note when shopping.

Use credit cards

Credit cards aren’t tied to your personal account so if you are unlucky enough to be defrauded the risk is minimised. Plus, credit card fraud, once it is proven, is often refundable. Debit cards on the other hand are not really covered. It’s largely up to your bank’s discretion as to whether they refund you. They are also tied to your bank account which could allow clever hackers to use your debit card details to plunder your account.

Use good online protection

This may seem as obvious as locking your front door when you leave home but you’d be surprised at the relatively large number of people who overlook this most fundamental cyber security step. Good internet security (https://www.bullguard.com/products/bullguard-internet-security.aspx) will negate many of the threats listed above. It flags up suspicious websites, malware that is hiding in emails, as well as keeping out a whole host of nasty viruses, worms, Trojans, spyware and other types of malware.

It always pays to be realistic when confronted with outrageously good offers such as flights to New York for under £30, an iPad for less than £50, the latest smartphone for £20, laptops for under £70 and so on. Online retailers are in the business of making money.

They don’t give stuff away; they assiduously watch what their competitors are doing to set their prices accordingly. As such they don’t throw goods at buyers; they carefully calculate their offers. They certainly don’t offer free money for simply redeeming a voucher as some Black Friday phishing ‘offers’ have claimed previously. So the more ‘outrageously’ good an online offer is the more likely that it’s a scam.

-ENDS-

About BullGuard
BullGuard (https://www.bullguard.com/) is a market leader in consumer cybersecurity. We make it simple to protect everything in your digital life – from your data, to your identity and your smart home. The BullGuard product portfolio extends to PCs, Macs, and Android tablet and smartphone protection, and includes internet security, comprehensive mobile security and 24/7 identity protection. BullGuard released the world's first IoT vulnerability scanner and leads the consumer cybersecurity industry in providing continuous innovation.

Dojo by BullGuard (https://dojo.bullguard.com/) is an award-winning intelligent cyber defence system and service that provides the highest level of protection to consumers across all of their connected devices and smart homes. Dojo is the cornerstone of a smart home, ensuring a connected world where every consumer in every home, is smart, safe and protected.

Privately held, BullGuard is based in Bucharest, London, Silicon Valley and Herzliya, Israel. Follow us on Twitter @BullGuard (http://www.twitter.com/BullGuard) and @DojoSafe (http://www.twitter.com/DojoSafe), like us on Facebook at BullGuard (https://www.facebook.com/BullGuard/?fref=ts) and Dojo (https://www.facebook.com/meetdojo/?fref=ts) or learn more at https://www.bullguard.com.
All trademarks contained herein are the property of their respective owners.

-ENDS-

Media Contacts:

Michelle Cross
The PR Room
Michelle.cross@theprroom.co.uk
+44 (0)333 9398 296

Sarah Chard
The PR Room
Sarah.chard@theprroom.co.uk
+44 (0)333 9398 296

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of The PR Room

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com