Article

Nov 2022

Don't buy more than you bargained for

The internet is the biggest retail park in the world and, despite originating in the US, Black Friday (and its counterpart Cyber Monday) has become the most anticipated shopping day* of the year.

Tom Lee
Information Security Consultant
Email tom.lee@waterstons.com

Every year many fall victim to retail scams, with British online shoppers defrauded out of £25m in the 2020 Black Friday period, with many imitation websites, or fake adverts on genuine ones fooling otherwise savvy bargain hunters to part with their cash.

With deals lasting all month in some cases, and many taking to the (virtual) shops during lunchbreaks, or even during work time, on company equipment, what measures can be taken to protect yourselves, your business and your equipment? Make sure your cyber resilience is tip top by:

1. **Conducting due diligence**

If you're purchasing from an unfamiliar website, carry out some research – look for online reviews, or a seller's feedback history before proceeding.

2. **Using a secure payment method**

Often websites have recommended payment platforms such as Apple Pay, Google Pay or PayPal, or use a credit card over a debit card as this offers buyer protection. Never pay for items online using direct bank transfer.

3. **Protecting your details**

Only complete what you need to and avoid creating an account, or saving payment details, unless you know and trust the website and are likely to use it regularly.

4. **Securing your accounts**

Use strong passphrases made of three random words for each of your email and online shopping accounts. If the website allows, activate two-factor authentication which gives your account additional security when logging in. For further information about how to secure your accounts, visit www.cyberaware.gov.uk.

5. **Being phishing aware**

Never click on a link in an unsolicited text or email - go to the website directly instead. Phishing attacks usually offer a deal that's too good to be true, or incite a sense of urgency – two things shoppers expect and fall victim for during Black Friday especially.

Phishing emails can be reported by forwarding the email to report@phishing.gov.uk and phishing text messages can reported by forwarding the original message to OFCOM via 7726, (which spells SPAM on your keypad). Finally, suspicious websites can be reported via the National Cyber Security Centre's scam website reporting service.

With sales countdowns, limited time offers, stock restrictions and must-have items being the focus, it's easy to lose your head during the Black Friday sales – just remember:

- **Stop:** Take a moment to think before parting with your money or information
- **Challenge:** Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040. If you're in Scotland, you can report it to Police Scotland on 101.

If you or your team encounter any suspicious activity over Black Friday, or you are concerned about potentially being a target, get in touch with our team of cyber security experts who can help build your business resilience.

(*weekend, week, month!)