



How to reduce Black Friday Cyber fraud/scams

This Factsheet has been created by Mazars in Ireland exclusively for IoD Ireland members.

To get staff to understand the importance of cyber security, you must get personal, and tap into the ‘what’s in it for me’ principle. Mazars outline below a few tips to raise staff awareness of the threats of Black Friday online shopping.

Ahead of one of the biggest online shopping events of the year, **Black Friday** on 27 November and **Cyber Monday** on 30 November, scammers are ramping up their activities.

Many retailers kicked off their Black Friday deals early from fashion and beauty to household goods and toys, looking to increase online sales where lockdown measures have impacted traditional in-store purchases.

Cyber-crime risks span across generations; anyone can be the target of financial fraud and scams and at any time. The Banking and Payments Federation of Ireland (BPMFI) recently reported figures that overall **card fraud reached €22 million in 2019**. With these statistics in mind and a significant increase in online shopping, **consumers best defence is to stay informed, alert, and secure.**

Warning signs to be on the lookout for:

1. Online shopping scams using a fake website that looks legitimate offering products at low prices, using unreliable payment methods;
2. Fake adverts posted on a classified website; and
3. Non trustworthy product offers sent via emails and text messages to shoppers.

Personal information is valuable. There's a lot to lose, beyond euros and dollars. It can take years to recover an individual's identity if affected by fraud and scams. There are some simple ways for online shoppers to protect themselves:

- Don't trust a website or an advertisement just because it's advertised on social media, classified website or it's endorsed by a celebrity.
- Do your research on the website or seller's history and reliability, checking independent reviews will help verify authenticity.
- Only shop with an online retailer where the 'https://' and locked padlock symbol is displayed in the website address.
- Only make a payment with secure payment methods like credit cards and PayPal.
- Don't click on links in unexpected emails or messages, even if it appears to have come from a legitimate source.
- Avoid online shopping on public networks or Wi-Fi connections where your data will be less secure.
- Keep an eye on bank and credit card statements for purchased items you don't recognise.

If you suspect your personal data has been compromised via online shopping, contact your local authorities or bank immediately.

Contact Sarah Hipkin, Director in Mazars for details on how to deliver effective cyber policies, training and awareness, that tailor cyber security culture to how people behave online, at home and at work.

For more information please visit:

www.mazars.ie/Home/Services/Consulting/Risk-consulting/Cyber-behavior-culture



Sarah Hipkin

Director Mazars in Ireland

shipkin@mazars.ie

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.ie