opinion

Stay in the know about Christmas shopping scams

The festive period is a busy time of year for us all, including cyber criminals. Read on to find out about some key online scams to watch out for this Christmas period and help yourself to stay safe:

FAKE WEBSITES

- Check website URLs, spelling, functionality, and image quality.
- Still unsure? Search for the retailer on a new browser tab and compare the URL.
- Buying from a new or smaller brand? Make sure to check Trustpilot review pages.
- Check seller reviews if you're buying from an online marketplace.
- Be aware of hard to find goods 'suddenly' becoming available.

FALSE ADVERTS ONLINE AND ON SOCIAL MEDIA

- Have a healthy scepticism about the adverts you see online and on social media.
- In 2020, consumer advice site 'Which?' managed to promote a fake brand and fake health advice to highly targeted audiences on Google and Facebook. Ouch!

'BANK' EMPLOYEES CALLING

- Getting calls from your bank? Be cautious this Christmas period.
- Do they need you to do something immediately? Do they need your password or PIN to confirm you're the account holder?
- Unsure? Hang up and call your bank on the number on the back of your card.

NEW AND EMERGING SCAMS

- A recent Whatsapp scam where criminals pose as family members or friends, asking individuals to transfer them money, has been on the rise.
- Almost £50,000 has been lost between August and October of this year.
- Check the Action Fraud and NCSC websites for more updates like these.

inside out COMMUNICATIONS CONSULTING

insideoutconsulting.co.uk/cybersafe

Cyber Safe