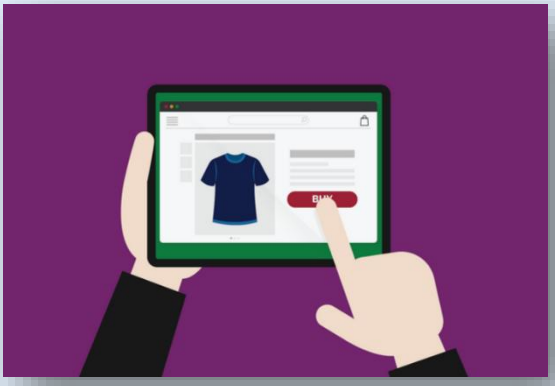
Cyber Byte

November 2025.

‘Authentication’

“The process of determining if someone (or something) is who (or what) it claims to be…”

We are fast approaching the time of year when we will begin to receive increased numbers of emails, texts and social media, advertising deals for all sorts of products.



In amongst this cyber enabled influx, will most likely be scam emails, texts and fake reviews, sent out in huge numbers by cyber criminals attempting to scam us.

November traditionally marks the starting point for many people to begin Christmas shopping and Cyber criminals have also been preparing their scams for this busy time of year.

These scams will include a mix of links to dodgy websites and “to good to be true deals” along with last-minute offers on limited stock, perhaps with a sales pressure message ***‘limited stock, 25 people have purchased this item in the last twelve minutes***’

Of course not all advertising is fake, but if something doesn't feel right, if you have that element of doubt as to the authenticity of the email or text you can get support from Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK

It is also extremely important you do your research to ensure the retailer is genuine. If you're unsure, don't use the link provided in the email, text or social media review but do a product search yourself.

Reputable retailers will have many consumer reviews, read these reviews as they will inform your decision to either deal with that retailer or not.

You should also consider your online payment method. Most credit card providers protect online purchases and by using a credit card rather than a debit card means that if your payment details are stolen, your main bank account won’t be directly affected.

The NCSC have provided excellent guidance to support your Shopping and paying safely online - NCSC.GOV.UK

If you've received a suspicious **text message**, forward it to **7726**. It won't cost you anything and allows your provider to investigate the text and take action (if found to be a scam).

When you are browsing and perhaps visited a **website** you think is trying to scam you, you can easily this using this link Report a suspicious website - NCSC.GOV.UK

What can you do to protect yourself from fraud this Christmas?

- **Protect your online accounts:** use different passwords for your accounts. Use Three random words - NCSC.GOV.UK to create a strong and memorable passwords, and enable 2-step verification (2SV).
- **Do your research:** make sure you do a thorough online search before making any big financial decisions. Check the authenticity of the company or organisation before making any investment, donation to charity or booking tickets for a concert, event or holiday.
- **Avoid paying by bank transfer:** you shouldn't be pressured into transferring large sums of money. A genuine organisation will not force you to transfer money on the spot, only a fraudster will try to rush you.
- **Scammer will use unsolicited emails, texts, QR codes and social media reviews:** advertising unbelievably good deals on items, always double check the authenticity of the retailer and what you are going to buy online, before making a purchase or paying upfront fees.

You can also visit Cyber Aware - Cyber Scotland for additional guidance.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.