We are fast approaching the time of year when you will now probably start receiving many emails from online stores, due in part because we ‘opt in to

Cyber Byte

November 2022

‘Authentication’

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

Cyber scammers are preparing…… to get the most out of you this Christmas!!

We are fast approaching the time of year when we will begin to receive emails from online stores and other retailers advertising deals for all sorts of products. This mainly due in part because we have ‘opted to receive notifications’ from them.

However, in amongst this influx of genuine emails, there will most likely be the scam emails, the fake ones, sent out in huge numbers by cyber criminals wanting to scam us.

November marks the starting point for many people to begin festive shopping and as much as we are preparing and looking at online deals, be in no doubt that the scammers are prepared with a mix of scams.

These scams will include phishing emails and texts with links to dodgy websites and to cheap “to good to be true deals” and last minute offers on limited stock, perhaps with a sales pressure message ‘10 people have purchased this item in the last five minutes’ all in an attempt to scam you of your money.

Of course, not all messages are bad, but if something doesn't feel right, if you have that element of doubt as to the authenticity of the email, text or website, follow the NCSC guidance on dealing with suspicious emails and text messages:

It is also extremely important to do your research and to ensure the retailer you are dealing with is genuine or not. If you're unsure, don't use the link provided in the email or text, but search a website address yourself. Reputable retailers will have many consumer reviews, read these reviews as they will help you make 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 online securely - NCSC.GOV.UK

Received an **email** which you’re not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at report@phishing.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). Visited a **website** you think is trying to scam you, report it to the NCSC

Information from Police Scotland Cybercrime Harm Prevention Team
PPCWCyberHarmPrevention@scotland.police.uk

All information correct at time of distribution. 01/11/2022