IT'S THE COUNTDOWN TO CHRISTMAS!

Stay Cyber Aware

WITH THESE TOP TIPS:

Be Wary Of Suspicious Links

- Avoid clicking links in emails that are from unfamiliar senders.
- Research retailers you're not familiar with and look for reviews.
- Look out for fraudulent emails - check email addresses against others you received in the past.

Don't Rush, Don't Be Pressured

- Use known reputable websites, especially for sales events.
- Don't rush to buy a product, even if it is from a legitimate company - you could regret it and then struggle to cancel/refund it.
- Products marked 'limited stock' or 'last few remaining' are sometimes a lure to make you rush into a purchase and could potentially be a scam.

Use Strong Passwords

- Use 3 memorable but random words together.
- Use at least 12 characters and add numbers and special characters at the start, middle or end to increase it's strength.
- Use unique passwords for each of your important accounts such as social media, email and websites storing banking details.

Make Sure Websites Are Secure

- Check for "https://" in web addresses or a locked padlock symbol in your web browser.
- "https://" doesn't necessarily mean the website is legitimate but it does mean the connection between you and the website is encrypted.
- "https://" doesn't guarantee that your information can't be intercepted but it is definitely better to have it than not.

Use A Guest Account On Websites

- Try to reduce the amount of online accounts you hold, particularly ones containing personal and financial information.
- If you aren't using a website frequently, checkout as a guest rather than making an account.
- Keep your personal information to a minimum to reduce the amount of information available to criminals if the website is hacked or suffers from a data breach.

Check Your Bank Statement Regularly

- Regularly check your bank statements for payments made that you don't recognise.
- If you find any transactions that you were not aware of, contact your bank immediately.

IT'S THE COUNTDOWN TO CHRISTMAS!

Stay Cyber Aware

WITH THESE TOP TIPS:

Complete Transactions Through Official Websites

- Be wary of a seller asking you to pay by bank transfer or outside of a website.
- Payment services like PayPal or using credit cards offer additional protection.

Be Careful With Adverts On Social Media

- Don't click links on advertisements. Check reputable websites for products and reviews.
- If in doubt about the authenticity of a website, don't give any personal or financial information.
- Schedule and run anti-virus scans regularly. If you think you may have visited a suspicious website, run a scan.

Keep Your Documentation

- Legitimate companies will usually send you an order confirmation.
- Keep your documents safe until you are happy with your purchase.
- If the product you have ordered comes with a guarantee, keep the receipt, and submit any forms offering guarantees or free servicing.

Research Businesses and Products Before You Buy

- There are plenty of reputable review websites online, and some merchants have their own feedback facility.
- Keep an eye out for similar looking language used in multiple reviews for the same business or product; this can be an indicator of a scam.

Secure Your Devices and Apps

- Make sure your devices have up-to-date anti-virus software installed and turned on. Both Apple and the latest Microsoft computers come with anti-virus pre-installed.
- Your computers, devices and software will often notify you of updates. Don't ignore them, install them at the earliest opportunity.

Secure Your 'Smart' Devices

- Change default settings on your smart devices. Usernames and passwords should be changed if possible.
- Keep an eye on available updates and security fixes from the manufacturer. Some devices won't automatically update.
- If you decide to get rid of/sell your device, remember to perform a factory reset to return it to original settings and remove your data.