TOP CYBER SCAMS IN 2021

Templar Executives
Cyber Security Resilience For Business

ONLINE SHOPPING

Online shopping "bargains" that were too good to be true **cost shoppers £15.4 million** over Christmas 2020. Look out for fake websites, and always make purchases directly from the retailer's own website, to avoid scams.

ROMANCE

From April 2020-21, romance scams **increased by 40%.** Total losses stand at £73.9 million and on average, victims make 5 payments to the malicious actor. Report anyone suspicious who is repeatedly asking for money to **Action Fraud**

SOCIAL MEDIA

Scammers post malicious links on popular social media platforms and persuade others to like and share - **only share genuine content.** To confirm this, hover over the URL to see if it redirects to a legitimate site and check the branding.

HEALTH

The Omicron Covid variant is used in phishing emails to encourage payment for 'new' test kits and to steal personal and financial data. **The NHS will not ask for your bank details or for personal documents.** The NHS website: **https://www.nhs.uk**

TOP TIPS

- ✓ Always have **anti-virus** installed and running when online.
- ✓ **Do not provide personal or financial data** without checking the authenticity of the website/person.
- ✓ Check the **padlock sign and 'https'** are in the URL when you are on a website.
- ✓ Download software and apps from **legitimate sources**.
- ✓ Set up **2 Factor Authentication (2FA)** for online accounts.

DELIVERY

In October, **81% of scams were a SMS message claiming to be from a delivery firm.** Royal Mail accounted for 62% of the cases, DPD 19% and Hermes 15%. Always check with the company before clicking on the link and giving away personal data.

JOB OFFER

On average, 2/3 of people search for jobs online and **lose £4,000 each to job scams**. Be suspicious if the contact does not use a company email and check legitimacy via websites such as **Companies House** and **Overseas Registries**

E-CARD

E-Cards are a convenient way to send best wishes to family, friends and colleagues. Cards that contain an attachment or a link could contain malware – **watch out for poor spelling and grammar, and an odd or unknown sender name**.

BANKING

2021 has seen a rise in vishing (voice phishing) scams - fraudsters call victims claiming to be from their bank and ask for their banking credentials. Don't be pressured and **call your bank directly to confirm the validity of the claim**.