Have yourself a cybersafe festive season

While we begin to wind down for the festive season, cyber criminals are gearing up to take advantage of the huge increase in online shopping, social media activity, seasonal travel – not forgetting our more relaxed mindset!

Here are our top tips for staying safe online during the festive season.

Phishing and Social Engineering

- Beware of phishing emails purporting to be from companies like Amazon and DPD. These usually contain links to either fake websites that aim to harvest your credentials or personal information, or to malware laden attachments. If you’re unsure, don’t click on the links! Login to the provider’s website and check your delivery status there.

- Be on the lookout for fake SMS or emails claiming to be from your bank or credit card provider. Never log in using a link sent in a text or email. Always navigate directly to the website, or use an official app.

- Even if you do everything right, a compromise may be outside your control. But by using a strong and unique password for every account, you can prevent hackers doing further damage.

For further guidance, see our guides on Phishing, Social Engineering, Malware, and Passwords.

Holiday Travel

When travelling away from home to be with family and friends, don’t let your guard down.

- Ensure your devices are locked and encrypted and only connect to trusted networks.

- Make sure you protect your personal data when travelling.

- If your office or home will be empty over the holiday period, make sure doors and windows are locked and use alarms and CCTV where possible.

- Before leaving work for the holidays, take time to secure paperwork containing sensitive data.
Devices

Many of us will receive a new device as a Christmas gift.

- Take time to double check all available security settings to make sure it is as protected as it can be.
- Ensure parental controls are in place on devices belonging to children or younger relatives.
- And don’t forget to take care when disposing of old devices. If reselling, seek expert help for wiping data first.

For further guidance, see our guides on Personal Devices and Remote Working and Physical Security.

Protect yourself and others online

Make sure you’re using those new devices responsibly.

- Be mindful of overshar ing in online games and social media, you may give away enough info for an attacker to steal your identity.
- Never share your travel plans publicly online.
- Be aware of your digital footprint. What you say and do online will likely be recorded by service providers and/or other members of the online community.
- Finally, be watchful of vulnerable users who may be potential victims of cyberbullying and harassment. Make the most of account privacy settings and report any issues you see.

For further guidance, see our guides on Social Media, Digital Footprint, and Cyberbullying and Harassment.