cosurica

Staff Holiday Cybersecurity Checklist

Stay safe online while you're away – protect yourself and the business.

1. Before You Go

Out-of-Office Reply

- □ Use different messages for internal and external contacts.
- □ Keep external replies short – no dates, names, or locations.
- □ Example: "I'm currently unavailable and will respond on my return."

Device Prep

- □ Update software and security patches.
- □ Turn on multi-factor authentication (MFA).
- □ Encrypt devices (laptops, tablets, phones).
- □ Set auto-lock after short inactivity.
- □ Back up important files.

2. While You're Away

Phishing Awareness

- □ Be suspicious of unexpected travel-related emails/texts.
- □ Don't click links or open attachments unless verified.
- □ Report suspicious messages to report@phishing.gov.uk or text 7726 (free).

Device Use

- □ Avoid public Wi-Fi – use a trusted hotspot or VPN.
- □ Disable Bluetooth and Wi-Fi auto-connect.
- □ Don't use public USB charging points.
- □ Keep devices with you, not unattended in hotels or vehicles.

3. If Something Goes Wrong

Lost or Stolen Device

- □ Notify IT/security immediately.
- □ Request remote wipe if possible.
- □ Change passwords for any accounts accessed.

4. Social Media & Privacy

- □ Don't announce your trip or post live location.
- □ Wait until you're back to share holiday photos publicly.
- □ Avoid posting boarding passes, passports, or hotel details.

Remember: Cyber criminals take advantage when routines change. A few extra precautions can prevent a costly breach.