**Quick Security Fixes**

**EMAIL:**

 Require strong, unique passphrases on email accounts

 Turn on two-factor authentication on sensitive accounts

 Encrypt sensitive emails and use digital signatures

 Do not use personal email accounts for company business

 Train employees to recognise phishing emails and avoid suspicious links or attachments

**MOBILES:**

 Delete unnecessary apps and update the rest regularly

 Only download apps from trusted sources and check reviews prior to downloading

 Secure with passcodes or biometric authentication, such as fingerprints

 Turn off Bluetooth, GPS and Wi-Fi whilst not in use.

 Turn on remote wipe and device encryption

 Configure app permissions after downloading

 Do not connect to unknown public networks - use a VPN.

**Wi-Fi**

 Physically secure Wi-Fi equipment

 Change default admin password, the name of the SSID and SSID passwords

 Restrict remote administrative management

 Use a network monitoring app to scan for unwanted users and be mindful of signal radius

 Keep firmware updated

 Use separate Wi-Fi for guests and school users.

**SOFTWARE**

 Make sure the operating system, browser, and applications receive automatic updates

 Get rid of unused software

 Equip all machines with regularly updated antivirus software

**3RD** **PARTY** **VENDORS**

 Set out privacy and security expectations within the contract

 Put in place procedures to check vendors are following security rules set

 Limit access to systems and data on a need-to-know - temporary - basis.

 Enforce multifactor authentication from remote locations

 Establish procedures for the reporting of incidents and the sharing of intelligence

**RESILIENCE**

 Determine the most important operations and the systems they depend on

 Develop work arounds for when IT systems are offline

 Ensure regular backups are tested, encrypted and stored offline.

 Ensure IT have priority checklists to isolate problems, sanitise, rebuild and restore systems

**USBS**

 Disable auto-run

 Scan USBs and other external devices for viruses and malware

 Allow only pre-approved USB drives and do not permit any others to be plugged in

 Ensure USBs benefit from encryption and avoid storing sensitive information altogether

**WEBSITES**

 Require users to create unique, strong passphrases to access

 Use vulnerability scanners to test your site’s security – many are available free of charge

 Consider Web Application Firewalls (WAF) and Database Activity Monitor (DAM) for added

protection as part of defence in depth.

**Reporting**

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or [online.](https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime)

Forward suspicious emails to report@phishing.gov.uk.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).