New Device Checklist: Employer Edition

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Laptops & Desktops

- [ ] Asset management - Ensure you've recorded;
- [ ] Device make, model & serial number
- [ ] Who is it assigned to & when was it assigned
- [ ] When should it be returned
- [ ] Does the device need to be installed onto your works network?
- [ ] Ensure firewalls and anti-virus software are enabled
- [ ] Ensure operating system updates are installed
- [ ] Ensure application and software updates are installed
- [ ] Make sure that physical and digital files are encrypted
- [ ] Make sure that you backup files daily/weekly
- [ ] Restrict the use and downloading of applications which aren't specific to their job role
- [ ] Ensure the user profiles are setup with the correct permission levels
- [ ] Review plugin device settings to ensure they are secure

New Device Checklist: Employer Edition

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Mobile Devices

- [ ] Ensure that all accounts have Two-Factor Authentication (2FA) enabled
- [ ] Ensure that all accounts are using strong passwords *(remember three random words)*
- [ ] Promote the use of a password manager to keep them secure and encrypted
- [ ] Ensure employees are making use of strong passcodes and Face ID
- [ ] Ensure application updates are set as 'Auto-update'
- [ ] Review all applications - if you want to restrict what employees can download, this should be covered in your company's Device/Security Policy
- [ ] Review the location settings - setup 'Find my iPhone'

Tips in the Office

- [ ] Offline/Cloud backups - ensure that devices are backed up on a regular basis, either daily or weekly.
- [ ] Security Policies - Ensure your staff review all of your company's security policies
- [ ] Cyber Security Policy
- [ ] Password Policy
- [ ] Working From Home Policy
- [ ] Device Usage Policy

New Device Checklist: Employer Edition

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Tips for working from home or remotely

- [ ] Ensure a paid VPN is in use when working remotely
- [ ] Always ensure that you use a unique email address AND password if you sign up for public WiFi
- [ ] Review the web address (URL) of any website you visit/use, ensuring that it is legitimate and where you expect to be
- [ ] Review and ensure each website you visit uses HTTPS by checking for the padlock icon on the left-hand side of the web address (URL)
- [ ] Employees should use a screen privacy protector, webcam cover and secure case for all devices
- [ ] Give your employees regular security awareness training
- [ ] Encourage employees to ask any questions when unsure of any emails/calls/texts they recieve
- [ ] Report spam text messages to **7726**
- [ ] Report spam emails to **report@phishing.gov.uk**
- [ ] Report suspicious website to the **NCSC**