New Device Checklist: Employee Edition

THE
CYBER
RESILIENCE
CENTRE
FOR THE **NORTH WEST**

Review your employer's security policies

□ Cyber Security Policy

□ Working From Home Policy

□ Social Media Policy

□ Password Policy

Passwords

□ Ensure you are using Face ID and Passcodes

□ Make sure of a Password Manager

□ Don't forget to use Two-Factor Authentication on all your accounts

External Devices

□ Do not use unapproved devices

□ Use of any USB or external hard drives should be limited to only ones that your employer has given you

□ Use only the mouse and keyboard that your employer has given you as it's been confirmed to be safe and used with your device

Remote Working

□ Use a VPN when working remotely

□ Be wary of public wi-fi networks - always have your VPN enabled

nwcrc.co.uk

We help protect businesses from online crime.

New Device Checklist: Employee Edition

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Software and Applications - Backups & Updates

- □ Setup automatic updates for applications, software and your operating system
- □ Remember to run regular backups of your data via the cloud or your company's network
- □ Only use company-approved applications and software

Personal Accounts

- □ Don't use your work email for personal accounts
- □ Be careful sharing photos and videos which involve work devices, sensitive data or projects you're working on

Data Exposure

- □ Worried your email may have been involved in a data breach? Check HaveIBeenPwned
- □ Setup Notify Me alerts on HaveIBeenPwned
- □ Don't save any financial details or credit card details
- □ Save any work related financial or credit card details within your password manager