HOME WORKING CHECKLIST

ARE YOU MANAGING YOUR CYBER RISK?

Brought to you by Assure Technical

CYBER ESSENTIALS

Get in touch with our cyber experts

Telephone: +44 (0)1684 252 770

Email: cyber@assuretechnical.com

www.assuretechnical.com

ASSURE technical

HOME WORKING CHECKLIST

ARE YOU MANAGING YOUR CYBER RISK?

CYBER ESSENTIALS

Follow our simple ten steps to ensure you are protecting your business when staff are working from home:

Have any questions about protecting your organisation?

Get in touch with our cyber experts

Telephone: +44 (0)1684 252 770
Email: cyber@assuretechnical.com

www.assuretechnical.com

1. Install Anti-virus

Anti-virus software must be installed on all devices to protect your business from both viruses and malware. Most operating systems now come with built in anti-malware capabilities but you should ensure that this is appropriate for your needs. Ideally your installed anti-malware software should update daily to protect against emerging threats.

2. Enable Firewalls

Create a buffer between your network and the internet to provide good protection from cyber attacks. Most computers will have built in fire wall functions which should be activated.

3. Update Operating Systems and Applications

All devices and all applications must remain updated at all times. Most devices and applications will prompt the user when an update is available and can usually be set to update automatically.

4. Strong Passwords & Two-Factor (2F) Authentication

Set strong passwords for user accounts and enable 2F authentication as an extra layer of security where available.

5. Secure Video Conferencing

Many popular free video conferencing services aren’t end-to-end encrypted and expose you to the risk of criminals accessing your calls by ‘snooping’. Limit this risk by always using meeting passwords and opting for services with enhanced security, configuration and privacy features.

6. Limit Removable Media Usage

In order to avoid data loss and limit exposure to malware, permit only sanctioned products and disable the use of all other removeable media. Ideally you should encourage alternative means of data transfer making use of available online tools and products.

7. Controlled Access to Corporate Systems

Virtual Private Networks (VPNs) allow home workers to securely connect to corporate networks and should be used where feasible. If a VPN is not available, you should ensure that workers have secured their home networks by changing router passwords from the manufacturer’s default to new strong passwords. This should also be carried out on other networked devices such as printers, scanners or smart TVs.

8. Personal Device (BYOD) Security

All of the steps listed above should be implemented on any personal devices that are used for business purposes. These should also be controlled and managed through an appropriate company policy.

9. User Education

It is vital that users are educated on how to keep their devices and software up-to-date and detect email scams. They should also be advised to maintain levels of privacy by switching device cameras and microphones off and keep their devices and company data somewhere safe when not in use.

10. Incident Management Procedure

There should be a clear and simple process for any user issues, for example when a device is lost or stolen, or a user accidently clicks on a suspicious email.