digital wholesale solutions

Power in Partnership

DAY IN THE LIFE OF A REMOTE WORKER: ARE YOU SECURE?

When you have employees working remotely, from anywhere, they are at risk of security breaches throughout the day. Are you doing everything you can to keep your business and data secure?

Check out our typical Day in the Life timeline to see where you could be leaving holes in your security approach and find out how to plug them.

9AM

9am: Employee logs on to their laptop

> Are they using the latest version of your VPN software?
> Did you know many data breaches could have been prevented by patched software?

Small Business Guide: Cyber Security

30% involved internal threat actors

10AM

10am: Employee receives a suspicious email, do they know what to do?

> Is your employee aware of “phishing” and how it could be used to plant ransomware or malware onto your network?

27% of breaches involved Ransomware

11AM

11am: Employee is waiting for a meeting in a coffee shop and is using their tablet

> Is there a privacy screen on the device, protecting what’s on the screen from anyone looking over the employee’s shoulder?
> If the device was lost, do you have a record of it on your asset register?

Managing network devices

12PM

12pm: Employee shares documents with a customer via an app installed on their mobile

> Do you have control over this information?
> Could you set up your own controlled file share system for large files?

Mobile Device Guidance

1PM

1pm: Employee is checking personal emails on their work device while at lunch

> Are uploads being monitored?

Improved patching has reduced vulnerability exploitation to **5%** of all breaches. **Keep patching!**

2PM

2pm: Employee needs to provision a service with a supplier – there is only one password in use for the company

> Would you be sure to change the password in the event that the employee left the organisation?

28% of breaches involved small businesses

3PM

3pm: Employee installs unauthorised software onto their device

> Are employees required to get authorisation for software downloads from IT to prevent malware being installed onto devices?

67% of breaches are caused by credential theft, social attacks and errors

4PM

4pm: Employee leaves their laptop on the train home

> Is it encrypted?
> Do you need to inform the ICO of a data breach? Are you aware that you have 72 hours to do this?

ICO Guidance

SME FAQs

Phishing

Phishing is a type of email attack where attackers attempt to trick users into doing the wrong thing, such as clicking a bad link that will download malware, or direct them to a dodgy website.

Malware

Malware is malicious software, which – if able to run – can cause harm in many ways, such as causing a device to become locked or unusable or stealing, deleting or encrypting data.

Ransomware

Ransomware is a type of malware designed to block access to a system or device until a sum of money is paid to the hacker.