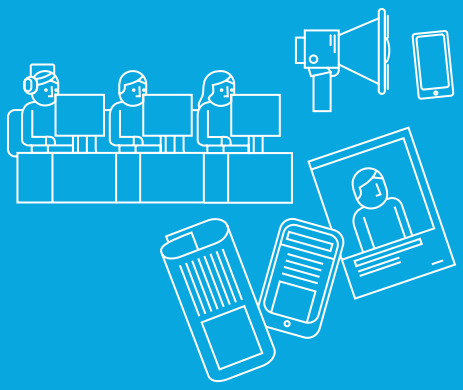
RSM'S **CYBERSECURITY** TOP TIPS

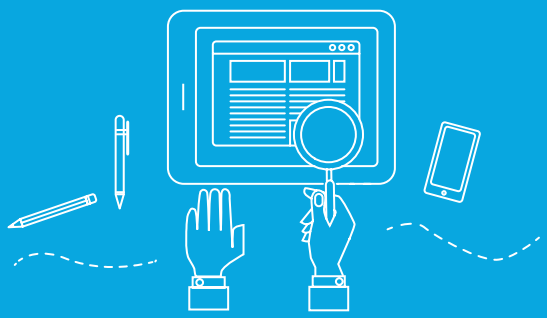


MAKE THIS A BOARD LEVEL ISSUE

- Consider all of your risks – data, people and third-party
- Review your policies and procedures
- Provide rolling education and training e.g. on the use of social media

STAFF RESPONSIBILITIES

- Read policies and procedures
- Keep up-to-date with education and training
- Be aware of unusual phone calls, e-mails or texts
- Verify contacts
- Accept all security updates to your PC/laptop as soon as possible
- Don't click on links – type in the URLs



CYBER RISK MANAGEMENT

- Report anything suspicious to IT immediately
- Be careful on social media
- Change your passwords regularly
- Have strong and different passwords for different accounts
- Be careful with portable media
- Check security certificates, especially for payment websites

WHAT DOES BEST PRACTICE LOOK LIKE?

- Keep your firewalls, operating systems, virus engines up-to-date
- Password protect the Wi-Fi
- Consider data scrubbing
- Implement good IT general controls in depth
- Have a formal Incident Management plan for when the worst happens
- Consider compliance with Cyber Essentials Plus, or similar good practice
- Consider cyber insurance
- Check physical site controls
- Review controls against social engineering generally
- Conduct penetration testing