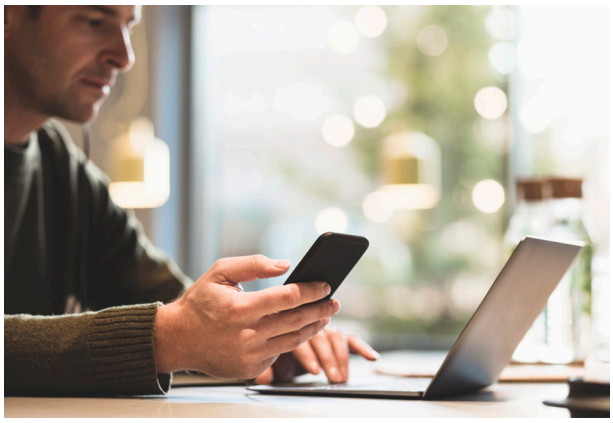
Risk Solutions

Being smart about your employees' devices

Mobility has enhanced business operations with many employees, particularly in SMEs, using their own smartphones and tablets for work. Yet, 46% of businesses have been exposed to a cyber-attack because of BYOD (Bring Your Own Device) and of these companies, 57% state that online services are at the core of the business*.



The impact of financial or data loss on these firms is potentially significant, so businesses must effectively limit the risk.

Understand device risk

Smartphones and tablets have become an integral part of business operations, however the amount of data stored on devices and how they link to the company network can cause vulnerabilities for businesses.

As employees generally use their work smartphones for personal use, or their own devices for work, they download a mixture of apps, which are targets for hackers. Utilising this link, they can infiltrate the company network. This has resulted in data being stolen or corrupted, financial loss or business downtime.

How to protect company smartphones and tablets from hackers

BYOD policy

Ensure that you have a policy in place, so employees understand the risk of using their own devices and the rules to which they must comply to safeguard the business.

Robust antivirus

Only allow devices to access company networks that have a company approved antivirus software installed. Studies show that 20% of smartphone users have had their devices infected with malware and those infected have risen 300% since 2012.

Lock your smartphone with a passcode

Passcode protection prevents unauthorised access. Devices can be configured to automatically lock after a certain period of time and employees should be encouraged to never leave any devices unattended.

Secure access to emails

Use secure access email applications like Good, that enables employee access and productivity without compromising security.

Encrypt mobile devices

Add an extra layer of authentication by encrypting mobile devices to protect data stored on smartphones and tablets.

Install or enable remote wipe capability

Devices are lost and stolen all the time. Ensure you have a process in place for employees to report lost/stolen devices and agreement that their phones can be remotely wiped if stolen, protecting any data held on it.

Keep devices up-to-date

Ensure employees install the latest updates to keep devices secure, as well as enabling devices to perform at an optimal level.

Ensure apps and emails are from trusted sources

Be cautious when installing new apps or opening emails from unknown sources. These are easy routes in for hackers.

* Department for Culture, Media & Sport. Cyber Security Breaches Survey 2017. April 2017

Made possible
QBE

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 **QBEurope.com**

QBE European Operations is a trading name of QBE Insurance (Europe) Limited and QBE Underwriting Limited, both of which are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

8583/JAN/2018