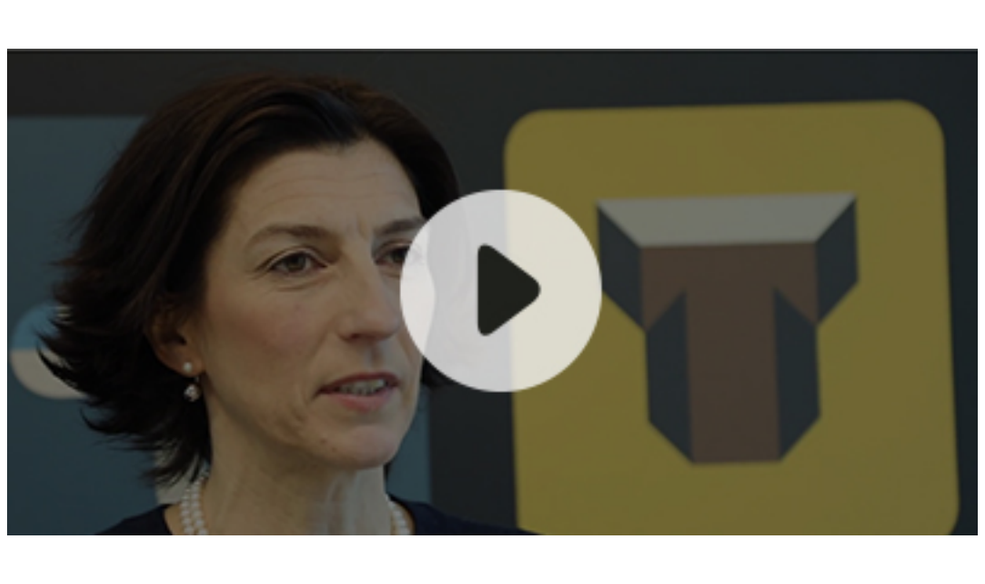
Businesses on the move

How Irish Businesses can Adopt Mobile Working and Maintain Security

Three.ie

Scroll to view content

Mobile working is both the new opportunity and the new challenge for businesses in Ireland. Digital natives demand it. Productivity is enhanced by it. Is security compromised by it?



Firm's favourite

1/3 of Irish firms forced to choose between their phone and their laptop as their only business tool would opt for the smartphone. More than three-quarters feel they can stay on top of their workload with just a smartphone.

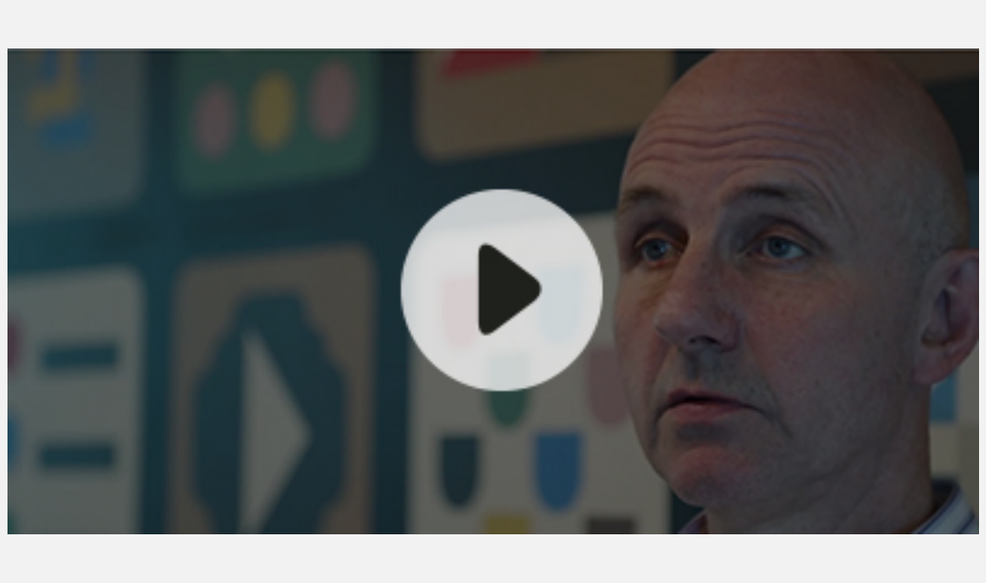
Mobilising productivity

85%

of Irish professionals claim workplace productivity is on the rise due to increasing use of laptops, smartphones and tablets.

Failing to manage

32%



of Irish businesses lack the technology platforms and support solutions to effectively manage mobile working.

10 tips for Securing Your Mobile Devices

Analysts predict that 25% of corporate data will bypass perimeter security and flow directly from mobile devices to the cloud by 2018. How can you make your data more secure?

1 Ensure Software Is Up To Date

Your device manufacturer will from time to time release updates with identified bug fixes and software enhancements. Keeping up to date with releases ensures you are protected from the latest threats and have the newest features.

2 Lock Your Device

Lock your phone with a password or fingerprint detection. Try using a sentence as your password, it's easier to remember. Set the time on your password lock to be short as well - 60 seconds or less.

3 Encrypt

If not turned on by default on your device, consider encrypting your device. Doing so will protect sensitive data, whether its business data or just your photos.

4 Be Careful With Free Wi-Fi

Be cautious what you do while using free Wi-Fi, it may not be secure. Try not to carry out banking transactions or transmit sensitive data when connected to them.

5 Backup

Always backup everything stored on your mobile device that is of any importance to you - files, photos and contact details. Secure automated backups will mean the world to you if your device is lost or stolen.

6 Avoid Third Party Apps

If you're on an iPhone, you don't have much of a choice. For Android users however, staying on Google Play and not allowing apps from unknown sources keeps you relatively safe. If you do decide to use third-party apps, be "app aware". Read reviews, and if the app asks for access to too much personal data up front, don't download it.

7 Stay Away From Jailbreaking And Rooting

Avoid jailbreaking your iPhone or rooting your Android. While the processes are different, the end result is bypassing what phone manufacturers intended (including security protocols) and ultimately weakening the security of your device.

8 When in Doubt - Don't Respond

Fraudulent text messages, calls and voicemails are on the rise. Remember, requests for personal data or immediate action are almost always scams.

9 Seperate Accounts

It's best practice to have a second or even third email account for registering for mailshots, websites, etc. If possible, try not to duplicate passwords from account to account. In 2011, the infamous Dropbox hack resulted in tens of thousands of usernames and passwords being compromised. Because people had used the same username and password combination for multiple different services, all their other accounts were compromised too.

10 Manage Your Devices

Employ an effective Mobile Device Management solution throughout your entire fleet of company and personal devices.

When everywhere's a workplace

A mobile workforce is still your workforce, and your workforce is your responsibility. However, changes in the way people work can also demand changes in the way you manage them.

Nurturing digital natives

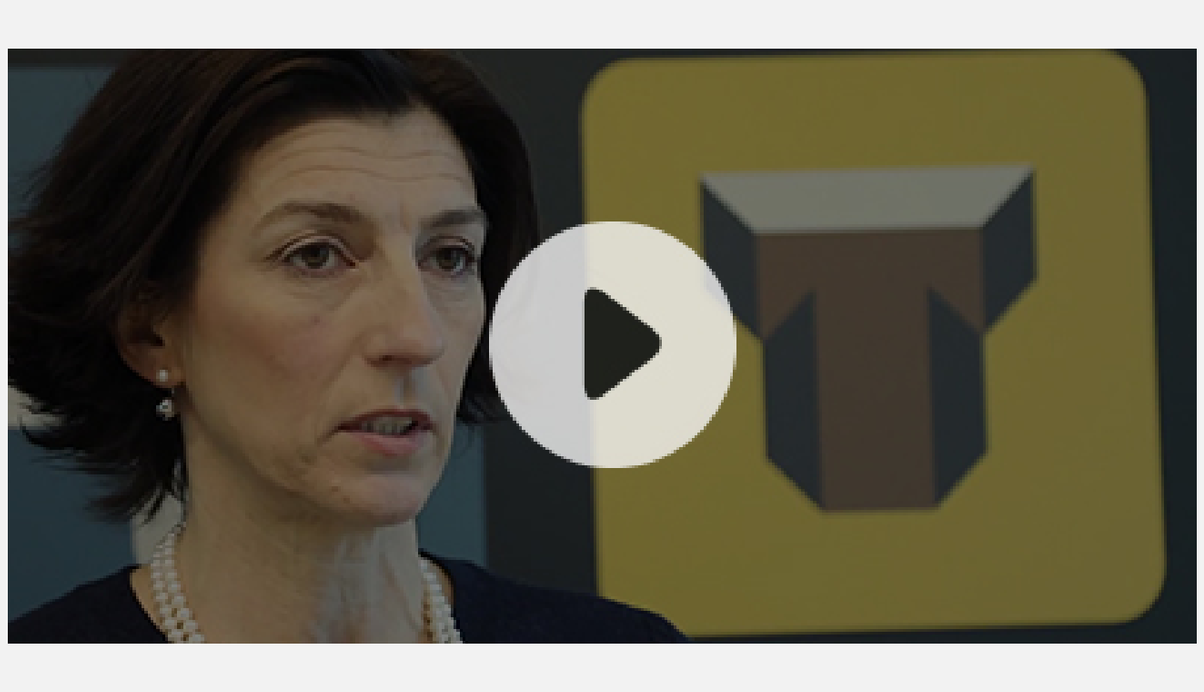
The current generation entering the workforce sees mobility as a necessity. If you want to attract and hold onto them as employees, you need to think the same way. An effective technological infrastructure for mobile working is one aspect. An appropriate attitude towards mobility and workplace flexibility is another.

Building trust

Managing a virtual team of mobile workers demands a different set of management skills. Building trust amongst management and instilling accountability amongst employees is essential to effective mobile working. Cloud-based reporting tools can help create transparency. Performance - or output-based management – rather than a clocking-in and out/ 9-5 approach becomes critical.

Bring Your Own Device

Ireland has the highest penetration of phone internet users anywhere in Europe, North America or South America. They'll have their personal phones with them as they work, and may even use them for work. It's essential you have a security policy in place which covers, defines or prohibits personal devices and their use.



How Cork City Council moved to mobile

Read the case study of Cork City Council's successful, secure management of over 300 smartphones and tablets used by their employees.

Read Case Study

Want to move forward with mobility in your business?

Talk to a mobility expert from Three Ireland.

Request a call back now

Use the Communications Evaluation Tool to assess your current situation and your future requirements.

Use Communications Tool

Watch the 2017 Planning Webinar from Three Ireland to help you assess and plan your business priorities for the rest of the year.

Any questions? We welcome them.

Three.ie