

Mobile porn and Facebook seen as biggest productivity and security threats to mobile working

Survey reveals IT directors continue to suffer from lack of visibility over employee mobile usage

Results:

- 200 IT directors surveyed said that mobile social networking was the biggest threat (55%), followed by mobile porn (30%), mobile gaming (8%) and mobile TV (7%)
- 92% said that as more employees are using mobile devices to work remotely and access corporate networks, the number of security threats had increased
- Nearly two-thirds of IT directors admitted that they found enforcing mobile usage policies a headache.

Dublin, Ireland – 16th June 2010 – Damovo, the business communications provider, today announced survey results which reveal that social networking and mobile porn are the biggest productivity and security threats to mobile working. 55% of the IT directors surveyed said that mobile social networking was the biggest threat followed by mobile porn (30%), mobile gaming (8%) and mobile TV (7%).

These emerging threats are likely to grow as mobile working continues to rise in popularity thanks to the advances in mobile technology. 92% of respondents stated that as more employees are using mobile devices to work remotely and access corporate networks, the number of security threats they faced had increased. At the same time 95% of respondents admitted that their organisation's workforce was going to become even more mobile over the next 10 years.

"While this survey was undertaken in the UK, we are seeing very similar results in the Irish market," said Mary Bradshaw, managing director, Damovo Ireland. "As mobile devices become increasingly ubiquitous for business users in Ireland, it's important to be aware that inappropriate usage can introduce a wide range of security and productivity concerns. This needs to be managed carefully so that the many benefits that mobile devices bring to a business are not lost."

Increasingly, many workers are only using one mobile device for both business and personal use which can make enforcing mobile usage policies difficult. In fact, nearly two thirds (63%) of IT directors admitted that they found enforcing mobile usage policies a headache. It is therefore hardly surprising that 88% also admitted that they would like better visibility of their employees' mobile usage in order to better manage costs and improve mobile security across their organisation.

Currently, mobile security is often left in the hands of the end users meaning that important company and personal data can be easily compromised if devices are lost or stolen. In addition, the onus is on the end user to return mobile devices to the IT department or the device manufacturer when software needs upgrading. As a result, organisations are left with many different devices running different software versions with differing levels of protection. 82% of IT directors believed that such inconsistent upgrade cycles were leading to increased mobile security and performance concerns. At the same time, 94% also believed that their mobile devices should be decommissioned in a more secure manner, considering the increasing amounts of sensitive personal and business data today's devices hold.

One of the main causes of these problems is that in a lot of organisations mobile devices are purchased through procurement or on a departmental level rather than through IT.

Unsurprisingly, 81% of IT directors admitted that they found it difficult to manage and secure their mobile phones when they were not purchased through or specified by the IT department.

“The latest mobile device management solutions can provide IT departments with far greater visibility and control over the mobile devices on their network. Features such as ‘over the air’ updates’, data encryption and remote data wiping can provide businesses with greater peace of mind that their workforces’ mobile devices are secure, especially if they fall into the wrong hands, “concluded Mary Bradshaw.

The survey of 200 UK IT directors at organisations with over 1,000 employees, was commissioned by Damovo UK and carried out by independent research company Vanson Bourne.

ENDS

About Damovo

Part of the Damovo Group, Damovo Ireland is a leading provider of unified communications solutions and services in the enterprise arena. It has 30 years experience delivering and supporting complex communication networks and integrated business applications across Northern and Southern Ireland. Damovo has key strategic partnerships with leading technology vendors in the market, such as Aastra, Cisco, Mitel, Extreme Networks and Microsoft. Damovo Ireland has more than 400 customers in the public and private sectors. These include Enterprise Northern Ireland, the University of Ulster, CIE, ESB, Bord Gais, The Revenue Commissioners, The Courts Services, HSE, Dublin Institute of Technology, Trinity College Dublin, and Hertz.

For more information visit www.damovo.ie

For more information, contact:

Barry Chapman

Comit Communications & Marketing

t: +353 1 215 7671

e: bchapman@comitmarketing.com

w: www.comitmarketing.com