

## **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*

**Horsham, UK – 14 June 2010** – Research released today by enterprise ICT solutions and service provider, Damovo UK, has revealed that social networking and mobile porn are the biggest productivity and security threats to mobile working in UK businesses. 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.

“Sophisticated mobile devices are becoming the de-facto tool of choice for business users, yet it is clear that this is also bringing a whole raft of security and productivity concerns,” said Alex Donnelly, Portfolio Manager at Damovo UK. “Without properly provisioning and having an effective mobile device management strategy in place, organisations are going to incur increased support costs and risk losing the visibility and security they had created in the fixed desktop environment.”

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.

“It is clear that IT should play a key role in the procurement of mobile devices, as it is best suited to the role from a cost, security and management perspective. 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 also means that IT departments can have greater peace of mind that

their workforces' mobile devices are secure, especially if they fall into the wrong hands," concluded Alex Donnelly.

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 UK ([www.damovo.co.uk](http://www.damovo.co.uk))**

Damovo is an established ICT provider and integrator with over 30 years' experience – from IP-enabled connectivity, infrastructure and desktop to fixed and mobile devices and multimedia applications whatever your communication requirements. From supply only to a fully outsourced solution, our services cover the spectrum of consultancy, design, implementation, support and lifecycle management.

Damovo partners with over 100 technology specialists, holding the highest levels of accreditation with Microsoft, Aastra, Cisco Systems, Extreme and Mitel.

As part of the Damovo Group Limited, which has operations in ten countries, Damovo UK has more than 600 clients spanning 5,000 sites. Clients include Mersey Care NHS Trust, Bournemouth University, Manchester United, Transport for London, Nutricia, Bank of England and Imperial College Healthcare NHS Trust, North Ayrshire Council and University of St Andrews.

**For further information, please contact**

Alex Crawshaw / Ana Williams

Spark Communications

Tel: +44 (0)20 7436 0420

[alex@sparkcomms.co.uk](mailto:alex@sparkcomms.co.uk) / [ana@sparkcomms.co.uk](mailto:ana@sparkcomms.co.uk)