

GFI Software Survey: 100% of Commuters Put Company Data at Risk Over Free Public Wi-Fi

Submitted by: GFI Software

Tuesday, 17 September 2013

Commuter study reveals commuters regularly connect to free, unsecure Wi-Fi services during their daily journey, putting personal and company data at risk every week

London, UK – 17 September 2013 – GFI Software™ (<http://www.gfi.com/>) today announced the findings of an extensive independent research project looking at end user use of mobile devices at work and in their daily commute to and from the workplace, which revealed that commuters are using free, unsecured and unknown Wi-Fi services for accessing sensitive company data in greater numbers.

The survey of 1,001 UK office workers with a tablet or smartphone who travel to and from work on a train, bus or tube was carried out by Opinion Matters for GFI Software, and revealed not only that mobile devices and using data services are firmly entrenched as the primary activity of the average commuter, but also that commuters and their employers are falling foul of data security issues, as well as heightened risk of physical crime.

100% of the survey respondents acknowledged that they used open, public Wi-Fi connections at least once a week to carry out work-related tasks such as sending and receiving email, reviewing and editing documents and logging into other company servers and storage repositories. On average, users connected to public Wi-Fi to do work and access work systems 15 times a week, putting company data and passwords at risk from packet sniffing and other forms of traffic interception.

“The research findings reveal a stark and concerning trend among commuters – one of using their personal devices to catch up on work during their commuting downtime, but doing so over highly insecure internet connections that can be easily intercepted by other users or the operator of the access point,” said Walter Scott, CEO of GFI Software. “Mobile internet access is now firmly entrenched as a day-to-day norm, but with that has come an increasingly relaxed user attitude to data security, compliance and data governance policy. Companies need to address mobile device management to ensure that use in insecure environments doesn’t create vulnerabilities that could be exploited by criminals – both cyber and conventional.”

Key findings

- 46% use Wi-Fi as their primary means to access the internet on their mobile device, more than those who rely on 3G data services (43%).
- Only 7% of those surveyed are using 4G mobile data services as their primary way to access the internet on the move.
- 31% of respondents connected to public, untrusted Wi-Fi services to access confidential work data at least once a week, with the overall average being 15 times a week.
- 57% are concerned about being robbed if they use their smartphone or tablet in public locations such as train stations, bus stops or while walking to and from work.

- 52% of commuters are concerned about data being intercepted when using public Wi-Fi, but continue to use the service.
- Half of those surveyed become frustrated if no free public Wi-Fi is available, illustrating how users now perceive public Wi-Fi as a necessary part of daily life.
- 20% of mobile devices have no security enabled, not even a password or PIN number, while only 5% have corporate security policies enforced on their devices.

Mobile Device Crime

While crime on London's public transport system is down overall, muggings and thefts in and around tube stations and bus stops are on the rise. Figures released in August 2013 (<http://www.standard.co.uk/news/crime/tablets-and-smartphones-fuel-tube-crime-jump-8757035.html>) show that the overall number of offences jumped by a thousand, or 6.5 per cent, to a total of 17,030 in 2012/13, fuelled by a big surge in thefts of mobile phones and tablets.

The issue has been exacerbated by last year's launch of public Wi-Fi services on most Tube stations platforms and ticket halls. The GFI research data shows this is a popular and well-used service, with 84% of Londoners (against a national average of 87%) surveyed confirming that they openly use their mobile device on public transport, with 37% using free public Wi-Fi available at stations. The knock-on effect of this is that such services, as well as being unsecured, encourage users to openly display and use valuable computing devices in public, making them and their users increased targets for opportunistic thieves as well as cyber criminals. Commuters and pedestrians being targeted for their smartphones by muggers on bicycles is the capital's fastest growing crime spree according to police data.

From Commuting to BYOD

The survey also revealed that the increased commuter use of smartphones and tablets is pushing more companies to adopt Bring Your Own Device (BYOD) policies, often without the infrastructure in place to manage them. Only 5% of those surveyed had corporate security policies pushed out to their mobile device, while over a third (36%) admitted to using mobile devices to circumvent existing network security policies.

Use of personal mobile devices in the workplace is significant, with 100% of respondents using their mobile device for work and personal activities while connected to the company network. 27% of respondents spend between 20 minutes and one hour a week using their mobile device for work activities in the workplace, while 20% spend two hours or more. On contrast, 28% spend between 20 minutes and one hour a week using company Wi-Fi for personal tasks, while 17% spend over an hour a week using company Wi-Fi connections for personal activities on their mobile devices.

"BYOD is something that isn't going to go away. From the early days of executives buying PDAs and expecting IT to support them, end-user devices in the workplace being used for work tasks has been with us for over two decades. However, the explosion in BYOD fuelled by powerful and affordable smartphones

and tablets is such that companies have to manage it. Mobile Device Management is now a paramount IT security requirement for businesses of all sizes to maintain data security and integrity inside and outside of the company network,” said Scott.

The surprising ways people use their devices

A third (34%) of those surveyed also admitted to frequent use of their mobile devices while using the bathroom, an amusing result that goes some way to explaining why so many mobile phones suffer water damage and broken screens from being dropped into sinks and toilets. Women are the most prolific users of mobile devices in the bathroom and the bedroom, while men are the main users on public transport, at work and whilst walking.

The research found that 91% of women prefer to use their phone for conventional phone calls, versus 87% of men. Phone calls is still the most popular use for a smartphone, with 89% overall saying they make calls on the move. Only 16% use their devices for instant messaging and video calling.

A quarter use their devices for paying bills, 30% have replaced their morning newspaper or a book with a digital version on their device, 42% use it for shopping and for internet banking, 45% watch streaming and pre-loaded videos on the move, 58% play games and two thirds visit social networking sites.

However, only 31% actually use the calendar function on their smartphone or tablet to manage their diary, far lower than expected.

Overall, 80% spend their commute performing idle web surfing over any available internet connection, while 85% are sending and receiving email, firmly illustrating the volume of data that is sent around over a mixture of secure and insecure connections each morning and evening rush hour.

###

About GFI

GFI Software™ develops quality IT solutions for small to mid-sized businesses with generally up to 1,000 users. GFI® offers two main technology solutions: GFI MAX™, which enables managed service providers (MSPs) to deliver superior services to their customers; and GFI Cloud™, which empowers companies with their own internal IT teams to manage and maintain their networks via the cloud. Serving an expanding customer base of more than 200,000 companies, GFI’s product line also includes collaboration, network security, anti-spam, patch management, faxing, mail archiving and web monitoring. GFI is a channel-focused company with thousands of partners throughout the world. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

For more information

GFI Software

Please email David Kelleher at David.Kelleher@gfi.com

GFI - Malta: Tel: +356 2205 2000; Fax: +356 21382419

URL: <http://www.gfi.com>

Davies Murphy Group

Please email Chris Green at gfi@daviesmurphy.com

Tel: +44 1256 807362

Disclaimer

Copyright © 2013 GFI Software. OS X is a trademark of Apple Inc., registered in the US and other countries. All rights reserved. All other trademarks are the property of their respective owners. To the best of our knowledge, all details were correct at the time of publishing; this information is subject to change without notice