

WhiteSparks

+44 (0) 844 247 4538

whitesparks@whiterockglobal.com

www.whiterockglobal.com

Volume 3, Issue 60: 31 August 2011

Smartphones: Users' Ignorance is the Biggest Threat

Spy Snaps: **More in the News**



Smartphones: Users' Ignorance is the Biggest Threat

As smartphones have become a more popular target for hackers, there is an extensive list of new techniques that are used to spy on phone calls and access personal data.

Last week, the UK's Channel 4 News looked into the methods that are much more advanced than primitive hacking techniques used during the recent NOTW phone-hacking scandal. The major threat looming over millions of people is that the information gatherer would listen to everything spoken on the phone, and would even take a photograph using the mobile device without its owner knowing about it.

The surge in attacks is driven by a growing number of particularly Google Android smartphone users. By clicking on an email link, which contains malicious code, hackers are able to access emails and bug phone calls, even while the targeted phone is on a standby. These codes introduce a back-door entry that gives an access to all information, including phone calls, emails and photos.

Several independent researches also support this major alert. For example, the anti-virus company McAfee has reported a 76% surge in malware aimed directly at Google's Android smartphones, warning that fake updates and novelty apps are used to comb through smartphones for personal details.

Furthermore, a new survey conducted by the Association of Independent Research Institutes shows that 2/3 of users have a smartphone with no password protection. More than 90% of users store personal data, such as photos, emails or contact details, on their mobile phones. 1/3 also save login information, such as PIN codes or passwords, for various services, including online-banking on their mobile devices.

However, curiously enough the majority of users say they are not concerned about phone security, with nearly 60% of people saying they feel "safe" from the threat of hacking. This is certainly a big misconception that may cost them dearly.

Raili Maripuu, WhiteRock Managing Director: These recent surveys are a clear indication that the personal and corporate awareness on the mobile phone security is extremely low. The companies should understand that their resilience to information gatherers is as strong as its weakest link, i.e. employees who use their mobiles for work purposes and are unaware of the threats.

[Read Full Story from Original Source...](#)

DID YOU KNOW?

Advanced Encryption Standard (AES) that is used to secure online transactions

and wireless communications, was cracked by Microsoft and the Leuven Catholic University in Belgium.

Source: [TechEye](#)



Spy Snaps: **More in the News**

Chinese website has been discovered selling data stolen by a new malware that monitors phone calls and messages on mobile devices and runs on Google's popular Android operating system.

[Read More...](#)

The US Energy drink distributor Innovation Ventures sued a rival company Aspen Fitness Inc. and its CEO for the theft of trade secrets through a former executive.

[Read More...](#)

British Intelligence Services were asked by the UK Government to spy on the people who organised this month's riots across the country. MI5 and GCHQ cracked the BlackBerry encryption and intercepted Twitter accounts in order to prevent the attacks by rioters on two prominent locations – Oxford Street and the 2012 Olympic site in London.

[Read More...](#)



INVESTOR IN PEOPLE

© Cope Whiterock Limited 2011 - Critical Information Defence® - SECM® - ISO9001 Registered Firm - Certification Number GB2000647

WhiteRock - A Bond of Trust