McAfee urges consumers to take careful “app-roach” at Mobile Expo Asia

SYDNEY, Australia, June 11, 2014 – With the rise in both mobile malware and apps designed to collect personally identifiable information, McAfee, part of Intel Security, warns mobile users to think twice before downloading apps.

McAfee’s security warning is a timely reminder as Mobile Asia Expo brings together industry leaders in mobile communications to address challenges and innovations facing the industry.

“In recent years, mobile and tablet devices have become the number one way in which we connect to the Internet, use social media sites, conduct online banking and make financial transactions on the go. McAfee has found that privacy-invading apps dominate the landscape, some containing malware, and many leveraging ad libraries to target unsuspecting app users,” says Sean Duca, Chief Technology Officer, McAfee Asia Pacific, part of Intel Security.

Apps and Privacy

Recent McAfee research shows that an alarming amount of mobile users are allowing apps to mine their personal data in exchange for use of the app. Over half (51 per cent) of users allow access their photos, 43 per cent to personal contact information and a further 38 per cent allow access to their phone’s contact list – sharing contact details for friends, family and colleagues.[1] McAfee also found that 82 per cent of apps track you, and 80 per cent of apps collect location information.[2]

“While most apps are completely safe to use, some apps have a covert mission – to collect and share information on users. It is because of this, we are worried about the level of personal information that users are naturally willing to share with apps without concern,” says Duca.

Apps and Malware

Recent reports have shown that, globally, 2.4 million new mobile malware samples were added in 2013, up 190 per cent from 2012.[3] Across the Asia Pacific Region, mobile users in India, Russia, and Japan encountered the most malicious code.[4]

One of the most common behaviours – shown by more than one-third of the malware – is to collect and send device data that can be used to build a profile of the mobile device owner’s behaviour. There’s also a high prevalence of acts commonly associated with device hijacking, such as making the mobile device into a bot and installing other, even more malicious malware.

“Just one malware infection could have a devastating effect on a user’s phone, blocking access to contact details, phone usability or it could be programmed to skim personal information without their knowledge. It could also impact other devices on a home or community network,” says Duca.

Free Mobile Security

To combat the dramatic rise in the number of malware targeting mobile devices and to make security a more integrated part of the consumer experience, McAfee offers a full-featured version of its award-winning McAfee Mobile Security, available at no cost in 30 languages.

The latest version of McAfee’s free security app for Android and iOS devices enables consumers to instantly run free privacy and security scans. This new version of McAfee Mobile Security now also allows users to easily remove apps that pose significant risks.

App Scams To Watch Out For

· Mobile Shopping Apps – Official looking shopping apps, including those that feature celebrity or company endorsements, could be malicious, designed to steal or send out your personal data. Criminals can redirect incoming calls and messages, offering them the chance to bypass two-step authentication systems where the second step involves sending a code to a mobile device.

· Mobile SMS Scams – FakeInstaller tricks Android users into thinking it is a legitimate installer for an application and then quickly takes advantage of the unrestricted access to smartphones, sending SMS messages to premium rate numbers without the user's consent.

· Gift Scams – In-app advertisements that offer deals on must-have items, such as the PS4 or Xbox One, might be too good to be true. Clever criminals will post dangerous links and phony contests to entice users to reveal personal information or download malware onto their devices.

McAfee Tips On Protecting Your Privacy

McAfee has identified key tips to help safeguard your privacy either via apps or online:

· Don't just give away your privacy. Look at the permissions apps ask for and don't download apps that ask for personally identifiable information (PII) or extra permissions beyond the ones the app itself needs.

· Beware of apps that scour your device for interesting information they should never share – such as 'users you may know', locations and friend's contact details to 'share updates'.

· Download McAfee Mobile Security – it's free for Apple and Android devices

ENDS

About McAfee

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://au.mcafee.com/

###

[1] McAfee Love, Relationships & Technology research, February 2014

[2] McAfee Mobile Security Report, February 2014

[3] McAfee Labs Threats Report, Fourth Quarter 2013

[4] McAfee Mobile Security Report, February 2014

Contacts

Kristoff Clark
02 8303 6464
mailto: kristoff@zing.net.au