For Immediate Release

Straits Interactive releases findings of Singapore's first Mobile Apps privacy survey

Findings of top 100 mobile apps reveal privacy concerns and security risks for organisations deploying mobile applications

28 October, 2015 - Straits Interactive, a leading PDPA specialist, today released findings of Singapore's first privacy survey covering mobile applications (apps). The findings suggest that mobile apps downloaded within Singapore collect excessive personal data. Such apps are also susceptible to privacy and security vulnerabilities, an area which may be exploited by hackers.

The three month long survey, which covered 14 categories of mobile apps on the Android platform, studied the data privacy practices of mobile apps from both developers and organisations, comparing them to a similar privacy sweep conducted by the Global Privacy Enforcement Network (GPEN) on mobile apps worldwide. Conducted jointly with Appknox, a company that provides an automated testing tool for application developers and enterprises to help in the detection and resolution of security loopholes, the survey also scanned mobile apps for privacy and security risks. The Personal Data Protection Commission of Singapore has been given a copy of the findings.

Key Highlights of the Findings

Straits Interactive looked at the types of permissions an app was seeking, whether those permissions exceeded what would be expected based on the app's functionality, and most importantly, how the app explained to consumers why it wanted the personal information and what it planned to do with it. The findings showed that:

- More than 89% of the apps request more than 1 permission compared to the global average of 75% (67% of these applications request more than five permissions)
- 58% of apps had excessive permissions based on sweeper's understanding of app's functionality
- 18% of the apps had no data protection policy or information, other than permissions
- 55% of the apps did not have adequate privacy information as the sweeper did not know how information would be collected, used and disclosed
- In terms of permissions, many of the apps surveyed require potentially sensitive information such as location information – 70% (compared to 32% global average); 29% requests permission to access the camera and 52% to the device ID.

Further analysis of mobile apps code

To drill down further into the security and privacy loopholes, Appknox did a code analysis of the apps concerned, covering basic coding practices, data flow and metrics which include OWASP or Open Web Application Security Project configurations. The top three risks discovered were:

- 69% - Remote Code Execution Through Java Script Interface (where a remote attacker can execute malicious code, extract all user data or load malware on the device)
- 61% - Broken Trust Manager for SSL (a TrustManager is what the system uses to validate security certificates from the server)
- 52%- Derived Crypto keys (Weak encryption technique)

Said Mr. Kevin Shepherdson, Chief Executive Officer, Straits Interactive, “The findings raise privacy concerns and security risks from organisations deploying mobile applications, especially on the Android platform. Many of these apps collect excessive information and customers or users freely give permissions upon installation, without fully understanding or being educated as to how their personal information will be used and that their mobile device is now vulnerable to hackers. These organisations and developers need to take privacy considerations seriously when designing and deploying mobile apps as the findings imply a competency gap in this area.”

The survey findings recommend that companies urgently address privacy and security vulnerabilities in the mobile apps deployed while calling for organisations to review their own Bring Your Own Device (BYOD) policies. The findings also encourage developers and info-comm professionals to develop the bilingual skills of privacy and security.

“As Singapore moves towards its vision of becoming a Smart Nation, companies developing or deploying apps for their customers and users will need to address and strengthen the privacy elements of their apps,” said Mr. Ken Chia, Principal, Baker & McKenzie.Wong & Leow. ”They may not realise the privacy implications of their actions and that they may be contravening the Personal Data Protection Act. There is thus a need to further strengthen privacy in the face of an open world and a good way to do that is to help our technologists understand how privacy and security work hand in hand.”

To address the growing need for organisations and individuals in the financial, health, IT, and security industries extend their knowledge about data protection in the areas of product development and risk management, Straits Interactive will be offering a certification programme administered by the International Association of Privacy Professionals (IAPP) called the Certified Information Privacy Technologist or CIPT. The CIPT credential is also ANSI accredited and is the world’s first and only certification of its kind worldwide. The course begins on November 27th and is hosted at Baker & McKenzie.Wong & Leow’s premises.

Companies interested in obtaining a copy of the survey and its findings at a nominal fee can contact Straits Interactive at 6602 8010 or email at sales@straitsinteractive.com.

#####

About Straits Interactive

Straits Interactive delivers end to end governance, risk and compliance solutions that enable a trusted business environment and responsible marketing, especially in the area of data privacy and protection. We help businesses achieve operational compliance and manage risks through a combination of cloud technology and professional services.
By adopting a life-cycle approach to operational compliance and risk management, organisations are able to:

- Assess risks and compliance status across various stakeholders
- Protect against these risks and implement controls via policies, practices or technologies
- Sustain compliance efforts through audits, training and ongoing monitoring
- Respond to queries effectively or incidents systematically

Our Software-as-a-service offerings include the SpiderGate Do-Not-Call Management System, Data Protection Management System and the Governance, Risk & Compliance System, all of which are supported by professional services that include advisory services, audits, and training.

Media Contact

Straits Interactive Pte Ltd
Angela Schooling
Marketing & Communications Director
Email: angela@straitsinteractive.com
Mobile: +65 98222625