**Banks Far Behind Cybercriminals in Protecting Data with Preventive Technology**

In a series of recent events, android users have experienced banking malware threats resulting in an increased risk of identity theft and financial ramifications. Two of the most recent incidents include a DDoS attack on mobile apps of Lloyds Bank Group and a banking Trojan for stealing online leaked money by an underground forum of hackers. These events call for an urgent need of action on part of banks to take appropriate steps for the improvement of their mobile app security. According to app security specialist Promon, banks are easy targets because of their negligence towards mobile security.

Cybercriminals are no more amateur hackers trying to crack random passwords. They include sophisticated and organized groups that perform large scale operations for financial gains. Banks are at the core of their interest. Just as technology is improving to introduce better security techniques, cybercriminals are also adopting creative ways to refine and upgrade identity theft, ransomware, malware and other techniques of online crimes.

Head of Communication at Promon Lunde Birkeland said: “What we are seeing now is a steady development of a thriving internet of malware – a place where cybercriminals can work on their skills, share tips and tricks and create a community that is seeing the financial sector as a highly lucrative target, with the mobile channel a rapidly growing area for exploitation. Despite this clear and present danger, banks and financial institutions are still failing to fully comprehend the scale of the threat on their doorstep.”

The banking Trojan named BankBot has already been found to target Russian Android devices with their bank details, SMS messages, device tracking, making calls, and stealing sensitive data such as financial cards information.

With smartphone penetration on the rise in UK, banks are going to face serious consequences if they do not take solid steps to strengthen mobile app security. With more mobile usage hackers will have more room to plan and launch their attacks. It is therefore important for banks to consider mobile app security as their own problem rather than to leave it for the operating system or device manufacturer.