



PRAIRIE VIEW A&M UNIVERSITY

A Member of the Texas A&M University System

April 26, 2010

OFFICE OF BUSINESS AFFAIRS MEMORANDUM No. FY10-71

Distributed via Campus Email

To: All Employees

From: Mary Lee Hodge
Senior Vice President for Business Affairs

Re: US Computer Emergency Readiness Team Alert

Today's advanced mobile devices are increasingly used in the same way as personal computers (PCs), potentially making them susceptible to similar threats affecting PCs connected to the Internet. Since mobile devices can contain vast amounts of sensitive and personal information, they are attractive targets that provide unique opportunities for criminals.

Spy software is available that works on most of the major part of smart phones, including Blackberry, Windows Mobile, iPhone, and Symbian-based devices. The following are some of the capabilities provided by this software

- Listen to actual phone calls as they happen;
- Secretly read Short Message Service (SMS) texts, call logs, and emails;
- Listen to the phone surroundings (use as remote bugging device);
- View phone GPS location;
- Forward all email events to another inbox;
- Remotely control all phone functions via SMS;
- Accept or reject communication based on predetermined lists; and
- Evade detection during operation
- Access all the information on the smart phone

SMS, MMS, Bluetooth, social media (like FaceBook and Tweeter) infected TIFF attachments, maliciously crafted FTP protocols, and synchronization between computers and mobile devices are examples of potential attack vectors that extend the capabilities of malicious actors.

The user's limited awareness and subsequent unsafe behavior may be the most threatening vulnerabilities for mobile devices. Some risk mitigating measures are:

- Maintain up-to-date software, including operating systems and applications
- Install anti-virus software as it becomes available and maintain up-to-date signatures and engines
- Enable the personal identification number (PIN) or password to access the mobile device, if available
- Encrypt personal and sensitive data, when possible

- Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi
- Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices
- Use caution when opening email and text message attachments and clicking links
- Avoid opening files, clicking links, or calling numbers contained in unsolicited email or text messages
- Avoid joining unknown Wi-Fi networks
- Delete all information stored in a device prior to discarding it; and
- Maintain situational awareness of threats affecting mobile devices.

We urge mobile phone users to make themselves aware of the risks associated with the manner in which they use their devices and to utilize all appropriate precautions.

xc: Dr. George C. Wright

MLH:pgs