



THE INKERMAN GROUP

Smartphone Vulnerabilities

Securing your personal and business data

June 2010

SECURING YOUR PERSONAL AND BUSINESS DATA

The use of smartphones in business is increasingly becoming ubiquitous due to the attraction of keeping connected to the office while on the move. Devices such as BlackBerrys and iPhones allow the roaming user to check email, use GPS mapping to find locations, connect to the Internet and of course, make phone calls. Unfortunately, this mobile functionality has a downside, risking delivering sensitive data into the hands of malicious agents who would otherwise be unable to access the office environment. There are a number of precautions that the user should take to ensure that their data is protected at all times.

KEEP YOUR PHONE IN A SECURE LOCATION

Lost, misplaced or stolen smartphones represent the primary threat to your information. Accordingly, it is essential to keep the handset with you or store it in a secure location when it is not in use. Digital forensics experts in possession of a smartphone handset can extract all information contained upon it, including contacts, calls log, pictures, Internet history, email and website accounts and passwords. On devices with GPS enabled, the user's regularly visited locations and routes can be mapped out. It is important to consider that smartphones are essentially miniature computers, containing the sum of our digital lives while being small enough to be lost down the back of a chair or left in a taxi. The Home Office's Design and Technology Alliance Against Crime suggests that a mobile phone is stolen in half of all robberies, and this becomes especially disturbing when it is considered that many people keep information on their smartphones that would easily facilitate identity theft and fraud. Even seemingly innocuous items such as calendars may allow thieves to identify when users are on holiday and target their houses for burglaries, and such cases have already been recorded.

- 90% of smartphone users in the UK do not secure their devices
- Over 50% have submitted credit card details via their smartphones
- 16% keep bank details or PINs saved on their phone

Source: Sunday Times

In the event of theft or loss, if you are on a corporate BlackBerry Enterprise Server (BES), you can request that your BlackBerry administrator remotely wipes your device clean, assuming it is still connected to your organisation's BlackBerry Server. If you suspect your device has fallen into the wrong hands, it is best to inform your BlackBerry administrator immediately. It is safer to restore data from backup than risk someone cracking your personal information. There is also remote-wipe functionality on the iPhone, available from www.me.com.

EMPLOY CAUTION WHEN BROWSING

As with a PC, it is unwise to shop online, open email attachments and perform such actions as checking your bank account on your smartphone without having the appropriate firewalls, anti-virus and anti-malware protections in place. Although incidences of viruses and malware infecting smartphones are often not widely publicised, they present a serious problem due to the increasing shift of motivation of such crimes away from fun and towards financial gain. The primary type of BlackBerry infection is spyware, malicious software that is able to intercept emails and text messages, and even remotely activate the phone and listen in on conversations. Other smartphones

are not immune, with viruses having been documented across most platforms, including devices running the Android operating system. In March 2010 the first self-replicating iPhone virus was discovered. Software, including operating systems, should be kept up to date, and due caution should be observed when browsing the Internet.

TAKE A CAUTIOUS APPROACH TO APPLICATIONS

The security of applications, or ‘apps,’ varies from platform to platform. While iPhone apps are generally low risk, as they are approved by Apple and operate in a closed environment, others, such as those used on devices using the Android operating system, can pose a danger to the user’s personal information. Apps should be approached with the same caution as any other piece of software, and only trusted programs from a verified source should be installed. Free apps should be viewed with particular suspicion, as a current trend is for hackers to make free copies of popular apps laced with spyware capable of a wide array of malicious actions aimed at compromising your device. A June 2010 report identified that around 20% of third-party apps available through the Android marketplace allowed third-party access to sensitive data, such as making calls and sending text messages without the owner’s knowledge. In an open marketplace, it is the user’s responsibility to choose their applications carefully.

PLATFORM COMPARISON

BLACKBERRY

BlackBerrys have robust hardware encryption technology, tight access control and numerous security settings that allow the user to determine the level of protection they need, including a well-developed enterprise-level management system. The platform is approved for use by the US and UK government, and enjoys the confidence of most of the corporate world. It is up to the BlackBerry administrator and the user to set the level of security on their device according to their needs, for example, the US Department of Defence has issued a 125-page manual outlining the settings that must be in place before a BlackBerry is approved for official use. Although BlackBerrys have been compromised by malware, spyware and viruses, the manufacturer, RIM, regularly issues security updates to address vulnerabilities.

IPHONE

The effectiveness of security measures meant to guard against malicious hacking attempts on the iPhone have been subject to some criticism. Indeed, UK government ministers have been formally banned from using iPhones after encryption and electronics experts at GCHQ refused to approve the device for secure official business. A March 2010 survey of 257 security professionals by nCircle revealed that 57% thought that iPhones presented the greatest smartphone security risk to enterprise, with Google’s Android in second place. The survey noted dissatisfaction with Apple’s approach of allegedly doing the “absolute minimum” to address enterprise security and supportability requirements, with no new iPhone enterprise security features since summer 2009, when hardware level encryption was introduced and almost immediately subverted.

The risk of installing malicious applications is reduced due to Apple vetting each app that is listed in its App Store, and this process largely eliminates the possibility of installing ‘phishing’ apps, i.e. applications that purport to be something they are not. ‘Jailbroken’ iPhones, those devices which have been cracked to allow unauthorised applications to be installed, do not benefit from this protection.

ANDROID

Smartphones using Google's Android operating system, a modified version of Linux, lack hardware encryption and have features that make them more vulnerable to security risks. Applications do not require digital signing, and can expose features such as the file system, meaning that Android devices can theoretically have their data compromised by software. One advantage is that applications have to explicitly declare what capabilities/data of the phone it wants to access/use, and the user has to explicitly allow it those permissions before it is allowed to install. This allows a well informed user complete control over what is installed on their device.

SECURING YOUR BLACKBERRY

Perhaps the most effective action you can take to secure your data is not to store or access anything of a sensitive nature on a BlackBerry you are intending to take out of the office. When this is not possible, there are several inbuilt security features that the user should be aware of.

- USE A PASSWORD

To set a password, simply go to **Options > Security, Options > General Settings** and set **Password** to **Enabled**. This password should be strong enough not to be easily cracked (include numbers and letters), despite the temptation to set a simple one for ease of access. You can also set how long the device will sit at idle before locking itself; it is recommended that this time is set to as short a time as is practical.

- SET NUMBER OF PASSWORD ATTEMPTS

If a password is typed incorrectly ten consecutive times, all of the information on the blackberry is automatically deleted. To set the number of attempts (between 3 – 10), from the **Home** screen click **Options > Password > set the Number of Password Attempts field > Menu Key > Save**.

- ENABLE CONTENT PROTECTION

If Blackberry Enterprise Server(BES) is utilised, data being transferred between handset and server is encrypted. By default, this is not the case with the data stored on the actual device, however enabling Content Protection will encrypt emails and other stored content, and prevent others reading the device's memory through external connections such as USB. To enable **Content Protection**, go to **Options > Security Options > General Settings**. Set **Content Protection** to **Enabled**. Applying Content Protection to the Address Book removes the Caller ID function, so it is up to the user to determine whether the risk outweighs the inconvenience.

- PASSWORD ENCRYPTION

The built-in password encryption/storage program 'Password Keeper' should be utilised as a safe way to store passwords on your BlackBerry. This password store can only be accessed using a previously set password, and is a more secure way to store passwords than using MemoPad or emails in your mailbox. It is not advised to store complete login data, as there is always the possibility that the program can be cracked and the data extracted.

- SD-CARD / MEDIA CARD ENCRYPTION

Media cards can contain photographs or tracking-logs that you may not want others to gain access to. The encryption mode for the BlackBerry's Internal SD-card can be activated at: **Options > Advanced Options > Media Card**.

- LOCKDOWN BLUETOOTH

Bluetooth is an efficient means of connecting to other devices for hands-free talking and interaction, however it also adds a potential entry point for malicious hackers. It is therefore advisable to disable Bluetooth functionality when not in use: On the **Home** screen > **Manage Connections** icon. Click **Bluetooth Options** > press the **Menu Key** > click **Options** > set **Discoverable** field to **No**. Press the **Menu key** > click **Save**.

- WIPE THE DEVICE BEFORE ABANDONING IT

Before selling or passing the device to another user, it should be wiped clean of information. The notable example of the dangers of not doing this was provided by the McCain Presidential Campaign in 2008, which sold several leftover BlackBerrys for US\$20 each, inadvertently including confidential campaign data. To wipe the device go to **Options > Security Options > General Settings**. Hit the **Menu Key**, then select **Wipe Handheld** and follow the prompts. The only way to be completely sure of permanently wiping information on the device is to destroy it.

SECURING YOUR IPHONE

Although the BlackBerry remains the most popular smartphone in use in the corporate world, the iPhone has taken the personal market by storm. This popularity makes the iPhone a priority target for those with malicious intent, and it is important to take appropriate security precautions to protect both the user and information contained on the device:

- ENABLE PASSCODE LOCK

Enabling Passcode Lock will prompt the user for a four digit pin code after the Auto Lock feature locks the phone. This can be defined under **Settings > General > Auto-Lock**. To provide further security, iOS 4, which was released in June 2010, allows an alpha-numeric password to be set, although this is not enabled by default.

- SET ERASE DATA OPTION

As with the BlackBerry, the iPhone features an Erase Data option which will erase all data on the device after ten failed Passcode attempts.

- DISABLE WI-FI UNLESS REQUIRED

Manually enabling and disabling Wi-Fi when required will save battery power, as well as reducing the risk of connecting to insecure wireless networks without your knowledge. It is also advisable to disable Internet Tethering, as should you lose the device, your data connection can still be used even with a Passcode lock.

- ENABLE SSL FOR EMAILS

Secure Sockets Layer (SSL) is a security standard for securing the transmission of data between two endpoints. You should ensure that your mail servers are using SSL to ensure that email content is not transmitted in plain text over the Internet.

- WIPE THE DEVICE BEFORE ABANDONING IT

Before selling or passing the device to another user, it should be wiped clean of information. To wipe the device go to **Settings > General > Reset > Erase All Content**. Note: To be completely sure of permanently wiping information, the device should be destroyed. The only way to be completely sure of permanently wiping information on the device is to destroy it.

AWARENESS IS KEY

The major risk to sensitive information stored on smartphones comes through user carelessness, rather than technological threats. By enabling the appropriate security functions, assuming that your smartphone is inherently insecure, and employing caution as to what services are accessed over it, the risk of others with malicious intentions gaining access to information on the device is greatly reduced. The primary danger comes from your smartphone being stolen or misplaced, as regardless of the security measures in place, a skilled person in physical possession of your device will be able to hack into the information stored on it. Accordingly it is advised to pay attention to where your device is at all times while on the move, and to store it in a secure location when not being used.

For businesses, adopting and enforcing a robust smartphone security policy is advised, so that procedures are in place to outline acceptable use and to deal with rogue smartphones that may contain sensitive enterprise or personal data. Awareness of the strengths and vulnerabilities of your chosen smartphone platform is also essential so as to mitigate the risk of malicious actors compromising the data contained upon it.

DISCLAIMER

The contents of this document and any attachments do not constitute any commitment by the supplier, except where provided for in a written agreement between you and the originator. Whilst we undertake to use all reasonable care and skill in providing these services to our Clients, we cannot accept any liability for any losses suffered by the Client, where we have exercised such reasonable care and skill. In any event, the supplier does not accept liability for any consequential loss or damage of whatever sort, however caused to or incurred by the Client, in acting or relying upon any information provided to it by the Supplier and our liability is restricted solely to the restitution of our charges.

OPERATIONS CENTRE
INKERMAN HOUSE 3-4 ELWICK ROAD
ASHFORD KENT TN23 1PF

T + 44 (0) 1233 646940
F + 44 (0) 1233 646840

enquiries@inkerman.com
www.inkerman.com

111A WALTON STREET
KNIGHTSBRIDGE
LONDON SW3 2PH

T + 44 (0) 20 7589 5338
F + 44 (0) 20 7589 5339

DX: 30206 ASHFORD
KENT

IM MEDIAPARK 8
50670 KÖLN
GERMANY

T + 49 221 55405202
F + 49 221 5540545

REG IN ENGLAND NO: 3085655
VAT REG NO: 787297952
CONSUMER CREDIT LICENCE
NO: 420332
DATA PROTECTION: Z6511514