Advanced Corporate Solutions

"Debugging" Specialists | www.acsolutions.co.za

# 10 Methods

## of preventing mobile malware

**1. Inform users about mobile risks**

A mobile device is a computer and should be protected like one. Users must recognize that applications or games could be malicious, and always consider the source. A good rule of thumb: if an app is asking for more than what it needs to do its job, you shouldn't install it.

**2. Consider the security of over-the-air networks used to access company data**

Generally speaking, over-the-air (i.e., Wi-Fi) networks are insecure. For example, if a user is accessing corporate data using a free Wi-Fi connection at an airport, the data may be exposed to malicious users sniffing the wireless traffic on the same access point. Companies must develop acceptable use policies, provide VPN technology, and require that users connect through these secure tunnels.

**3. Establish and enforce bring-your-own-device (BYOD) policies**

BYOD should be a win-win for users and companies, but it can result in additional risk. Ask yourself: How do I control a user-owned and managed device that requires access to my corporate network? Employees are often the best defense against the theft of sensitive data. Employees using their own mobile devices must follow policies that keep the business compliant with regulatory requirements.

**4. Prevent jailbreaking**

Jailbreaking is the process of removing the security limitations imposed by the operating system vendor. To "jailbreak" or to "root" means to gain full access to the operating system and features. This also

means breaking the security model and allowing all apps, including malicious ones, to access the data owned by other applications. In brief, you never want to have root-enabled devices in your company.

## 5. Keep device operating systems up to date

This sounds easier than it actually is. In the Android ecosystem, updates can be blocked a number of ways: by Google (which updates the operating system); by the handset manufacturer (which may decide to release updates only for the latest models); or by the mobile provider (which may not increase bandwidth on their network to support updates). Without the ability to update your Android OS, your device is vulnerable to potential exploits. Research mobile providers and handset manufacturers to know which ones apply updates and which don't.

## 6. Encrypt your devices

The risk of losing a device is still higher than the risk of malware infection. Protecting your devices by fully encrypting the device makes it incredibly difficult for someone to break in and steal the data. Setting a strong password for the device, as well as for the SIM card, is a must.

## 7. Mobile security policies should fit into overall security framework

IT needs to strike a balance between user freedom and the manageability of the IT environment. If a device does not comply with security policies, it should not be allowed to connect to the corporate network and access corporate data. IT departments need to communicate which devices are allowed. And you should enforce your security policy by using mobile device management tools.

## 8. Install apps from trusted sources; consider building an enterprise app store

You should only permit the installation of apps from trusted sources, such as Google Play and Apple App Store. However, companies should also consider building enterprise application stores to distribute corporate custom apps and sanctioned consumer apps. Your chosen security vendor can help set up an app store and advise which applications are safe.

## 9. Provide cloud-sharing alternatives

Mobile users want to store data they can access from any device, and they may use services without the approval of IT. Businesses should consider building a secure cloud-based storage service to accommodate users in a secure way.

## 10. Encourage users to install anti-malware on their devices

Although malware exists for iOS and BlackBerry, those operating system interfaces don't support anti-malware. However, the risk of infection is highest for Android, where security software is already available. Make sure all your Android devices are protected by anti-malware software.