10 good habits to help secure smart phones

It will be difficult for technology employees to control what users will do with their smartphone device - and also keep them from exposing business data from security threats.

***TipsMake.com* - Think of all smartphones as unregulated endpoint devices. User identification of these phones may be stolen, hacked or illegally shared. They may also be lost, stolen or someone borrowed from you. Device identification technology uses serial number information to help businesses connect a smartphone to a specific user. This helps create a waterline on the device and allows IT to disable remote devices and erase all important data.**

The use of smartphones as a business tool is becoming increasingly popular. Soon, smartphones will replace computers to become popular Web access devices worldwide. As an inevitable consequence, people will find less IT people to solve technology problems. Because mobile phones offer advanced smartphone technology, users will look to the phone manufacturer they are using, who can meet their individual needs, rather than reaching out to people. These firms hire sales.

The problem is that the smartphone platform is in an insecure situation, like mobile network endpoints are being exposed to all the bad news on the Internet. Whether used in a company or individual, the smartphone has the ability to 'walk' in and out of the network, out and through the firewall. It will be difficult for technology staff to control what users will do with their smartphone device - and also keep them from exposing business data from security threats.

A smartphone can access the network via a wireless access point, which is said to be a form of attack risk like other devices. The only difference is that a phone is less capable of running the latest anti-malware security software (if available).

The vulnerability to attack is getting bigger

The development of smart phones in enterprise environments creates new and growing risks in data loss or leakage, whether by theft, illegal access or improper transmission of information. France. Like any phone with an online connection, password and security permissions are important to protect network access at an access port. In addition, the increase in the number of important and exclusive data lost and leaked from email attachments and posting of FPT is sent from smartphones.

The content contained in the smartphone is also easy to be lost or stolen by the network access code, usernames and passwords are often unsecured or user placed them automatically log in. Customers who have " *jailbroken* " their phones face the risk of leaving their original passwords, and their phones are easily hacked.

Moreover, the same risk of 'harassing' computer operating systems can also attack smartphones when they are transmitted via email, media pages, games, screen backgrounds, and photos. photos, messages, tweets, audio clips, slide shows, or in some cases, they are transmitted via dishonest short URL pages.

Smart phones are a source of malware infection, focusing primarily on spam emails, phishing - online scams, pharming - a form of phishing - and pretexting - pretending to steal information from phone calls. . Because smartphones are increasingly taking up a lot of standing in everyday communication compared to computers, users are also at risk of increasingly facing fake files in everyday communication.

In addition, users do not easily detect signs when a website fails on the tiny screen of the phone. While the infection may not be obvious, even after the phone is attacked, the file contains malicious code that could infect the network's IP address from this unsecured phone.

In addition, the superiority of Web 2.0 interacts and the flow of information transmitted via smartphones is at risk of being transmitted through traffic transmitted from the wireless network. Some applications, such as video streaming applications, are difficult to control. Not only that, like web-based devices that use apps over the network, smartphones are a 'potential' channel in denial-of-service attacks.

10 good habits

The use of smartphones in businesses is increasingly demanding dynamic goods, the best security habits. Therefore, organizations should pay attention to the practice of good habits below, using the heienj technologies such as SSL VPNs and the new generation firewall with intelligent control application.

1. **Setting Policy for smartphones** . IT should identify and use a Smartphone use policy in businesses, even if it is difficult to enforce personal devices. For example, a Policy may encourage users to set a password that is highly secure when accessing their device; requires installation of anti-virus software and malware on the phone; require immediate notification to IT staff when a smartphone is connected to a lost or stolen corporate network .

2. **Think of all smartphones as uncontrolled endpoint devices.** The smartphone's ability to identify users can be stolen, hacked or illegally shared. They may also be lost, stolen or someone borrowed from you. Technology to identify devices using serial number information to help businesses link smartphones with a specific user. This will help create a watermark for the device and allow IT to disable the device remotely and erase all important data.

3. **Set up SSL VPN access when connecting sources.** Secure Sockets The Virtual Private Networking Layer (SSL VPN) provides a central SSL VPN port to verify and access encryption on the Web to online resources from a variety of smartphone operating systems (eg Windows, Symbian, BlackBerry, iOS and Android).

4. **Comprehensive scan of all smartphone use.** In order to properly protect online resources from attacks aimed at smartphones, IT should deploy Next-Generation Firewall - the next-generation Firewall - to help conduct thorough checks of all phone traffic. Intelligent through SSL VPN.

5. **Control encryption and decode smart phone traffic.** IT should be sure to encrypt the smartphone traffic when transmitting information between the device and the connection port using SSL VPN. In addition, IT must also be able to decode traffic to be fully scanned with DPI SSL, and re-encrypted traffic for use in future communications.

6. **Maximize firewall traffic** . To minimize impact on critical applications such as video conferencing, voice over IP (VoIP) and Web 2.0 real-time interactive applications, the new generation firewall platform needs to scan and prioritize traffic Smartphone in real time.

7. **Set up application traffic management of smartphones.** Smartphone users rely heavily on Web 2.0 applications and are particularly vulnerable. Smart management and application technology can extend the function of the firewall such as identifying, organizing, managing and reporting traffic using the application over the network.

8. **Set up secure wireless network access for smartphones** . Most smartphones today have Wi-Fi connectivity and they are also at high risk of being connected to an unencrypted Wi-Fi point. Safety when connecting to a wireless network should also be as important as when connecting to a wired network, using a smart firewall. For employees who connect to the corporate network from public connection points, IT should apply a secure solution to access local intranet SSL VPN and thoroughly check the outbound / outbound traffic.

9. **Manage VoIP traffic of smartphones** . Because VoIP is used more often as a communication tool in businesses, it increasingly takes up more traffic. VoIP traffic is easy to affect service quality. Smart state management applications can prioritize storage for important applications like VoIP, as well as limiting bandwidth-intensive applications, such as YouTube.

10. **Manage bandwidth traffic of smart phones.** Organizations need to protect the connection of Voice-and-Data that today's smartphones offer. In addition, they also need to continue to optimize the quality of service and bandwidth management, as well as prioritize important applications.

Finally, businesses that use smart mobile phones in their business should have a habit of using them more securely. Organizations can implement the measures introduced above with existing modern technologies, such as SSL VPNs and new generation firewall with intelligent application management utility. All of these things help users to use their smart phones with the best security, as well as avoid the loss of important data in case the device is lost, stolen or unauthorized access.