ICT GROUP
INFOSEC101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

January 16,2015 Release #299

--Begin Transmission--

How to secure your mobile workforce

Smartphones are standard business tools storing sensitive business information and enabling email on the move. This makes them vulnerable to attack from malware authors seeking out new ways to defraud users and steal confidential business data.

While mobile viruses and spyware remain a relatively small problem compared with the much larger amount of malware targeting Windows computers, the risks to business reputation, communication and continuity are becoming more serious.

Risks include data theft, disruption of mobile phone networks and the hijacking of phones to send unauthorized revenue-generating SMS messages.

Mobile devices can be infected in many ways including email, MMS, external memory cards, PC synchronization and even via Bluetooth.

Make sure your security policy includes a strategy for mobile devices, covering:

- ✓ Threat management—identification and removal of viruses, spyware and spam.
- ✓ Device access control and management enforcing a password policy and application management.
- ✓ Data protection—encryption of sensitive data on devices and remote data deletion.
- ✓ Network access control—controlling VPN connections across public networks, validation of devices when they connect to the corporate network.

--End Transmission--

Information Security: It's a Shared Responsibility

REFERENCES

http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en.pdf

--End Transmission--

Document Code: 2015ICT_15SECA042