Dec 23,2014 Release #298

--Begin Transmission--

How to stay safe on the move

Educate users

Don't underestimate the risks of data loss from unsecured laptops or removable media. Organizations should develop clear policies concerning the use of mobile devices.

Use secure password

Passwords are the very first walls of defense and should always be as strong as possible.

Implement additional security checks

Smartcards or tokens require you to enter additional information (e.g., a token code together with your password) in order to access your computer. With fingerprint readers, you need to confirm your identity using your fingerprint when booting up or logging in.

Encrypt all important data

If your data is encrypted, it will remain safe even if your laptop or removable media is lost or stolen. If you don't want to encrypt your entire hard drive, you can create a virtual disk to store confidential information securely.

Restrict plug and play

Plug and Play allows USB drives, MP3 players or external hard drives to connect to laptops automatically, making it easy for data to be copied. Instead, lock the computer so only authorized devices are allowed to connect.

Secure remote connections

It is easy for nosy individuals to eavesdrop on wireless networks in airports, cafes, hotels and other public places. Secure communications with your organization's servers by using a virtual private network (VPN) configured on each laptop or mobile device. Some applications and websites can also be secured through the use of SSL to encrypt communications.

--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: 2014ICT_15SECA041