

FEBRUARY 2007

Volume 2, Issue 2

## Protecting Portable Devices

### From the Enterprise Security Office

Many computer users, especially those who travel for business, rely on laptops and PDAs because they are small and easily transported. While these characteristics make them popular and convenient, they are also easily lost or ideal targets for thieves. It is important to make sure you secure your portable devices to protect both the device and the information contained on the device.

#### What is at risk?

If your laptop or PDA is lost or stolen, the most obvious loss is the device itself. However, all of the information stored on it is at risk, as well. The data are often far more valuable than the portable device itself.

We've all read about lost or stolen portable devices containing confidential or sensitive information. Even if there isn't any sensitive or confidential customer information on your portable device, think of the other proprietary information that could be at risk: passwords, emails, contact information, etc. Below are tips to help you secure and protect your portable device.

#### Steps to take before you leave the office

- **Password-protect your portable device** – Make sure that you have to enter a strong password to log in to your device. If possible use a “power-on” password. This prevents someone from booting up your laptop with a different operating system on a CD, floppy disk, or flash drive.
- **Have your laptop configured to boot from the hard drive first** – Forcing your laptop to boot from the hard drive first prevents someone from rebooting your laptop from another drive e.g. floppy drive, CD, flash drive.
- **Install and maintain firewall and anti-virus software** – Protect portable devices from unauthorized access and malicious code the same way you protect your computer when at work. Install antivirus and firewall software and keep them updated.
- **Be sure all critical information is backed up** – Portable devices should not be the only place important information is stored.
- **Remove information that is not needed** – Don't carry around sensitive and personal information on your laptop or other portable device that is not necessary to you or your work.
- **Store your portable devices securely** – When not in use, store portable devices out of sight and, whenever possible, in a locked drawer or file cabinet.
- **Record identifying information and mark your equipment** – Record the make, model and serial number of the equipment in a separate location so that if your portable device is stolen the information will be available to the authorities. Label your portable device with an asset tag or other identifying label.

#### Steps to protect data

- **Encrypt files or the full disk** – Encrypting files or using full disk encryption reduces the risk of unauthorized individuals viewing sensitive data.
- **Consider storing important data separately** – By saving your data on removable media and storing it in a different location (e.g., on a lanyard around your neck instead of in your laptop bag), you can protect your data even if your laptop is stolen. If you store data separately you should also encrypt any confidential or sensitive data on that removable media.

#### Steps to take when traveling

- **When traveling by car** – If it is necessary to leave a portable device in a car, lock it in the trunk or other location where it is out of sight. Never leave electronic devices in cars for extended periods during either very hot or very cold weather. Never leave the vehicle unlocked when unattended, even for a minute. Do not leave the portable device in the vehicle overnight.

- **When traveling by air or rail** – Always keep your portable device with you or as carry-on luggage. Watch your device carefully as it goes through the screening process – this is an opportune time for a thief to take it. Make sure you have your portable device with you each time you board or disembark.
- **In the hotel room** – If a room safe is available, lock the device with other valuables in the safe. If it does not fit in the room safe, ask the hotel staff for the use of the hotel safe. If this is not practical, store the portable device out of sight when you leave the room.
- **At conferences and trade shows** – Be especially wary at conferences, large meetings and trade shows. These are common venues for thieves.
- **Downplay your laptop or PDA** – There is no need to advertise to thieves that you have a laptop or PDA or that you have the latest, greatest features. This is the type of language thieves look for, to identify potential targets. Avoid using your portable device in public areas, and consider non-traditional bags for carrying your laptop.

#### Steps to take at home

- **Keep the portable device out of sight when not in use** – If it is not in plain sight, a thief may not find it.
- **Treat it as if it were cash** – Think of the laptop as \$1,500 in cash and protect it accordingly.

#### What should you do if your laptop or other portable device is lost or stolen?

- Report the loss or theft to the appropriate authorities as soon as possible. These parties may include representatives from:
  - Local law enforcement agencies
  - Hotel or conference staff
  - Airport or other transportation security offices
  - Your organization's security office or help desk. They can then inform the appropriate parties to help protect any services that may be at risk.

#### Sources:

Washington State Department of Information Services –

[http://www.dis.wa.gov/technews/2006\\_02/20060209.aspx](http://www.dis.wa.gov/technews/2006_02/20060209.aspx)

State of Iowa Information Security Office –

<http://www.secureonline.iowa.gov/newsletters/index.html>

Office of the California State ISO –

[http://www.infosecurity.ca.gov/Library/Awareness/Information\\_Security-Awareness.asp](http://www.infosecurity.ca.gov/Library/Awareness/Information_Security-Awareness.asp)

US-CERT – <http://www.uscert.gov/cas/tips/ST04-017.html>

US-CERT – <http://www.uscert.gov/cas/tips/ST04-020.html>

#### Brought to you by:



<http://www.msisac.org>