

Mobile Security

Often the information contained on a laptop computer is more valuable than the laptop itself. Consider the well publicized cases where laptop computers containing sensitive information were stolen from UC Berkley, FTC, Equifax, the Vereran's Administration and others. It is like losing a wallet (or a file cabinet) full of data.



**Which is more Valuable:
The computer,
or the data
it contains?**

Using your laptop to get work done away from your office or on the road is becoming widely accepted. But this rapid growth in laptop computing has made portable systems the target for theft

around the world. If your laptop computer is stolen, company information can be exposed, as well as your personal and financial information.

Laptop security can be broken down into three realms: physical security, access control/authentication, and tracking/recovery. In this pamphlet we'll cover some ways in which you can improve mobile computing security.



Information Services Department
Information Security Office
55 Lake Avenue North
Worcester, MA 01655

Phone: 508-856-8643
Fax: 508-856-5150
E-mail: ITsecurity@umassmed.edu
Web: <http://www.umassmed.edu/IS/ITsecurity>

University of Massachusetts Medical School

Information Security Awareness Series

Mobile Computing Security



**Security Starts with
Awareness for Everyone**

October is National Cyber Security Awareness Month

Topic of the Week: Mobile Security

Laptop theft is a serious threat to users of mobile computers.



The Value is in the Data

Many methods to protect the data and to prevent theft have been developed, including alarms, laptop locks (such as the widespread Kensington lock stan-

dard), and visual deterrents such as STOP security plates that are hard or impossible to remove thus killing the resale value.

Victims can lose hardware, software, and essential data that has not been backed up. Thieves also may have access to accounts and sensitive data due to credentials that have been stored on the laptop including internet browser cookies, cryptographic keys and stored passwords.

According to the FBI, losses due to laptop theft totaled more than \$6.7 million dollars in 2005. For the last seven years, laptop theft has been found to cause the second highest amount of financial loss, second only to damage caused by viruses (2005 FBI Computer Crime Survey).

Physical Security

- Avoid using computer bags: they make it obvious where the computer is. Try a padded briefcase or suitcase.
- Use a laptop security device. If you need to leave your laptop in a room or at your desk, use a laptop security cable to securely attach it to a chair, table or desk.
- Register the laptop with the manufacturer. This step will “flag” your laptop in case it is ever returned for repair.
- Always maintain sight of your laptop. It’s easy to lose track of your bags while going through airport security. Ask for a “hand check” of your laptop in order to avoid the X-ray machine.

Access Control

- If your airline requires laptops to be checked baggage (as some now do), then whole-disk encryption is absolutely necessary.
- Never store passwords on your computer. Never leave access numbers or passwords in your computer case. It’s like leaving the keys in the car. By the time you notice your device is missing, your accounts could be cleaned out.
- Encrypt your data on all portable computing devices. If someone gains access to the laptop, at least they won’t have access to the data contained on it.
- Enable BIOS passwords and use strong passwords.
- Disable infrared and Bluetooth data transfer ports when using the device in a public place.

Tracking and Recovery

Use tracking software to have your stolen laptop “phone home”. Computrace “LoJack for Laptops” is offered via the UMass IS Help Desk at 856-8643

If your laptop is stolen

- Change your passwords for email, web, database, or other applications to prevent unauthorized access
- Contact Computrace and local law enforcement (where it was lost) and UMass Asset Management
- Check recent backups in order to determine exactly what was lost (you do have backups, right?)



Information Services Department
Information Security Office

Phone: 508-856-8643

Fax: 508-856-5150

E-mail: ITsecurity@umassmed.edu

Web: <http://www.umassmed.edu/IS/ITsecurity>