

SECURITY - *Now ...more than ever!*

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News - Your mobile devices are at the top of thieves' wish lists!

Protect Your Mobile Devices

Many people now rely on cell phones, laptops, blackberries, and USB drives because their portability makes them a convenient way to stay in contact with home and work. The convenience of these devices also makes them an attractive target for thieves. This newsletter describes several precautions to help keep your portable devices safe and secure.



Physical Security Options

First, write down all of your devices' serial numbers (usually found under the battery) and service tags, if available, and store them in a safe location. These numbers can play a vital role in the recovery process if your equipment is ever stolen. The first line of defense against loss or theft of portable devices is to physically secure them. Remember to keep your mobile devices with you at all times. You may consider purchasing belt clips for cell phones and blackberries. Many USB drives include key rings or lanyards to wear around your neck.

For laptops, you may consider purchasing a lock or alarm. These security tools are often



equipped with a combination lock or keys. They can attach to stationary objects, such as furniture, to avoid theft.

There are also alternative laptop carrying bags that are styled differently which

may help your laptop go unnoticed.

In public places, always keep a watchful eye on your equipment. There is no need to advertise!

Another Layer of Protection

Despite the best physical security practices, your equipment may still be misplaced or stolen. The severity of the loss can be mitigated by complementing physical security with strong data security.

- Use strong password mechanisms or PIN numbers wherever possible. Some cell phones, for instance, come equipped with a lockout feature that requires the use of a PIN number to operate the phone when it is powered on.
- Avoid storing sensitive data on CDs, DVDs, USB devices, and laptop hard drives.
- Use privacy tools, such as encryption, to protect your sensitive data. However, be careful not to forget your passwords, or you may lose your data. Backup your data files to a secure network drive to ensure that you always have another copy. Install and maintain Anti-Virus and Firewall tools.

In the Event of Theft...

Depending on the circumstances and location of the loss or theft, report it to a law enforcement officer, hotel or conference staff, and your own IT staff. Knowing the serial numbers will help identify you as the owner, speed up the recovery process, and help catch the thief.



Questions or comments? E-mail us at eSecurity@state.de.us