Texas Department of Information Resources

CYBER SECURITY TIPS

Monthly Newsletter

Office of the Chief Information Security Officer

January 2008 | Volume 2, Issue 1

SECURING YOUR LAPTOP COMPUTER

Laptop computers are increasing in popularity for both business and personal use. Their portability makes them extremely convenient. However, laptop owners must also be aware of the security risks from the loss or theft of laptops and take proper precautions. The potential loss is twofold – the loss of the laptop itself and any personal, private, or sensitive information that it may contain.

While you can take steps to secure the data on your laptop by installing a firewall, updating your antivirus software, using strong passwords, and encrypting your information, it is also very important to physically protect your laptop. Laptops can easily be stolen from the locked trunk of a car, at an airport security checkpoint, at an Internet café, or even from a hotel room. Keep these tips in mind when you travel with your laptop:

- Secure your laptop when unattended – Attach the laptop with a security cable to something immovable or to a heavy piece of furniture when it is unattended. Devices are available that sound an alarm when they detect unexpected motion or when the computer is moved outside a specified range around you.
- Don't store your password with your laptop – Secure your laptop with a strong password, but don't keep the password in the laptop case or on a piece of paper stuck to the laptop. For more information on choosing and protecting your passwords, please visit the following resource: **http://www.us-cert.gov/cas/tips/ST04-002.html**
- Don't leave your laptop in your car – Don't leave your laptop on the seat or even locked in the trunk. Locked cars are often the target of thieves.
- Don't store your laptop in checked luggage – Never store your laptop in checked luggage. Always carry it you.
- Keep track of your laptop when you go through airport screening – Hold onto your laptop until the person in front of you has gone through the metal detector. Watch for your laptop to emerge from the screening equipment.
- Record identifying information and mark your equipment – Record the make, model, and serial number of your equipment and keep it in a separate location. Consider labeling the outside of the laptop case with your organization's contact information and logo.
- Use tracking software – Consider using commercial software that reports the location of a stolen laptop once it's connected to the Internet.
- Backup your files – Back up your files before every trip. If your laptop is lost or stolen, you will still have a copy of your data.

If your laptop is stolen:

- Report it immediately to the local authorities if it is your personal laptop.
- Report it immediately to your employer if it is your business laptop.
- Contact the laptop manufacturer. If the thief sends it in for repair, you can request to be notified.

If your laptop contained personal or private information that might be used by an identity thief, visit **ftc.gov/idtheft** for more information on what steps you should take.

LAPTOP AWARENESS

Laptop thefts have become a common phenomenon in both the private and public sector. The State of Texas has not been immune from adverse publicity in this area. In light of this current threat, users should take every opportunity to increase security awareness. **OnGuard Online** offers some helpful resources:

- The Federal Trade Commission (FTC) has published a brief *Laptop Security Report* available for viewing and download at **onguardonline.gov/laptop.html**. The report offers user friendly tips for protecting laptops from theft.
- A five minute related online laptop security quiz entitled *Mission: Laptop Security* is also available for users to test their knowledge and enhance their security awareness: **onguardonline.gov/quiz/laptop_quiz.html**

Please take the time to read the report and take the online quiz.

As a reminder, computer security incidents that are critical in nature, involve the loss or exposure of Personally Identifiable Information (PII), or which may have the propensity to propagate to other agencies, should be reported to DIR Security as soon as possible. Please visit **www.dir.state.tx.us/security** for more information.

ADDITIONAL RESOURCES

For more information on securing your laptop:

- **www.us-cert.gov/cas/tips/ST04-017.html**
- **www.scambusters.org/laptop.html**

For related information, please see our previously issued newsletters on *Telecommuting Security Risks* (**www.dir.state.tx.us/security/reading/200707cybersec.pdf**) and *Protecting Portable Devices* (**www.dir.state.tx.us/security/reading/200702cybersec.pdf**).

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by:
MS-ISAC
www.msisac.org

Powered by:
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
www.us-cert.gov

Distributed by:
DIR
Secure Texas
www.dir.state.tx.us/securetexas