

State of Nevada
Department of Information
Technology
Office of Information
Security

Virus Protection: Having anti-virus software is critical on all computers, but doubly so if you use a laptop as both your home and work computer.

Advanced Security Features: Consider purchasing advanced security features such as biometric login, remote delete software, and location tracking for recovery in case of theft.

For Questions or Help

Contact your Office of Information Security.

Key numbers

Helpdesk (775) 684-4333
Department of Information
Technology (775) 684-5800
Fax (775) 684-5846

E-mail

infosec@doit.nv.gov



Laptop Computer Security
Quick Checklist

- Lock it up.
- Hide it and ID it.
- Protect against spies.
- Avoid storing sensitive data. If that is not possible, encrypt it.
- VPN.
- Backup, backup, backup!
- Keep your anti-virus software up-to-date.
- Do not connect to a public wireless network unless absolutely necessary.
- Use biometric log-in, if possible.
- Purchase locator tracking software, if possible.



State of Nevada
Office of Information Security
400 W. King St.
Suite 300
Carson City, NV 89703

LAPTOP COMPUTER SECURITY

BROUGHT TO YOU BY:

**DEPARTMENT
OF
INFORMATION
TECHNOLOGY**

**OFFICE OF INFORMATION
SECURITY**



<http://infosec.nv.gov>

LAPTOP SECURITY

Laptop Computers

Laptop computers are convenient. Because they are portable and user-friendly they can be used almost anywhere -- in airport terminals, hotel rooms, a quiet nook in a convention center. Laptops today have such high performance and data capacity that many workers can keep all their documents and files on a laptop and use it as their primary computer at either a main or offsite office, or at home.

Security Risks

Managing the security risks associated with using and storing sensitive data on a laptop computer is a continuing challenge. The same qualities many employees find so desirable in a laptop computer also make the machines natural targets for thieves. According to Safeware Insurance Agency in Columbus Ohio, more than 600,000 laptops are stolen or lost every year, just in America. And when one is stolen, it's more than just an expensive piece of equipment that is taken.



Another drawback to using one laptop at work and home is that viruses or other malicious software that infect the home system may contaminate the corporate network.

Additionally, wireless networks available at airports, hotels, and other businesses present high security risks because they require you to disable any wireless encryption or access control on your laptop in order to connect to them. Any information you exchange is now sent unencrypted and your laptop may be subject to probes and scanning from other computers connected to the wireless network.

Mitigating the Risk

Physical Security: At home or in the office, laptops should be physically secured with a cable lock. Attach them to something too large to move or break. Cable locks are widely available on the internet and in computer retail stores. Most major laptop brands have a slot for a cable lock. When traveling with your laptop, **never leave it unattended.**

Hide It and ID It: Use a nondescript carrying case for your laptop, since an



obvious laptop case can attract attention in public places. On the actual laptop, use identification markings that are difficult to remove, and leave evidence of tampering if removed. Always record your laptop's serial number and other identifying information. **Never leave your laptop in your car!**

Protect Against Spies: If you must use your laptop in public, use a privacy filter to prevent others from seeing your screen. Ensure that your computer is protected from spyware and malware.

Data Encryption: Encryption is critical for stored data whenever that data is subject to compromise. In the case of loss or theft, encryption will not get your laptop back, but it will make your data less vulnerable.

Secure Your Link: Utilize your agency's Virtual Private Network (VPN) software whenever accessing your office remotely. This will protect your data from compromise during transmission.

Backup: Because the potential for loss of applications and data is greater with a laptop, extra diligence is required in accomplishing backups.

