

Power LogOn

Security for Laptops

Convenience

- Power LogOn allows the user to never have to remember or type any log on user names or passwords. Now, companies can implement strong password assignment policies along with convenient password management for their employees.
- Laptops can now use long, complex user names and passwords during Windows boot-up because the user does not have to remember or type in the information.
- Advanced hard drive data encryption programs can now easily be used by the employee because they don't have to remember or type in the decryption authorization key – it is stored on the Power LogOn smartcard. Power LogOn will automatically launch the program and insert the key.

Security

- Power LogOn offers double, two-factor authentication: First, something the user has (the Power LogOn smartcard) and something the user knows (the smartcard's PIN); Second, something the laptop computer has (the smartcard), and something the computer knows (the log on passwords stored on the smartcard).
- By combining complex log on passwords with hard drive data encryption software, the data on a stolen computer is irretrievable. Thus all the personal information is protected.
- If companies and government organizations use strong passwords and hard drive data encryption software, they are not required by law to inform their customers that sensitive information may have been compromised. This is a great savings to companies both financially and with regard to their reputation.

Portability

- Power LogOn software can be loaded on to an unlimited number of computers, because the user license is on the card not the software.
- Power LogOn cards are the same size as a credit card so they easily fit inside a wallet or purse.
- When Power LogOn card is removed, so is any access to users' passwords and the computer can automatically shut down.

Did You Know?

Laptop Theft is a Frequent Cause of Stolen Information

Causes of Laptop Theft

- Companies do not train employees on what is expected of them when they are out of the office with a company computer.
- Disgruntled employees are often found to steal laptops from employers.
- Employers do not effectively secure their workplace.
- Thieves are aware that most laptops do not have a computer-tracing device.
- Most laptops do not have an advanced encryption to deter thieves and protect data.
- Laptops and their data are very valuable to thieves and are easy handle.

Statistics

- According to VNU Business Publications, in May 2004 the NHTCU (National Hi-Tech Crime Unit) noted that laptop theft is a greater cost burden to businesses than viruses.
- According to IDG News Service, in May 2006 a laptop containing credit card numbers and personal data of 243,000 customers of Hotels.com was stolen from an employee of Ernst & Young Global Ltd.
- According to EPIC (Electronic Privacy Information Center), in May 2006 a laptop containing sensitive information on more than 26 million veterans and service members was stolen from the Veterans Affairs employee.
- According to Baseline Magazine, laptop theft was attributed to 59 percent of computer attacks in government agencies, corporations, and universities in 2004.
- According to Computerworld.com, a laptop containing over 65,000 Rhode Island and Massachusetts YMCA members debit card, credit card and Social Security numbers were stolen from a YMCA administrative office in Providence, R.I. in May 2006.
- According to Reuters, in July 2006 a U.S. government laptop containing about 133,000 drivers' and pilots' records and Social Security numbers was stolen from a government vehicle in Florida.