

## Compliments of [HOWE SYSTEMS](http://www.howesystems.com) We bring you the Top 10 Tips for Data Security

Tips are ranked with the most important first and rankings are based on the premise that prevention is better than the cure.

1. Backup your data and configuration files. This is your insurance policy.
2. Always have a bootable system restore disk available. Make or obtain from your preferred Operating Systems vendor. If disaster strikes you must be able to revert to a known good state.
3. Always have a rescue disk. This enables you to reset passwords including root or administrator passwords and also to gain control of a machine that is in a zombie state. If you can not get a rescue disk burn a copy of Knoppix (a live Linux distro). It is highly recommended that readers get a Knoppix CD.
4. Restrict physical access to machines. Why? If someone with a rescue disk has access to your machines, they can simply boot from a rescue disk and gain root or administrator privileges for that machine.
5. When you implement a new system ensure data integrity by checksumming files. This will provide a baseline for your system. Some files checksums should remain unchanged, others will change daily. The files that change daily are kept in separate directories or file systems. This way we can see if critical files have been modified without our knowledge. Tripwire is popular with Linux and Unix users.
6. Implement hard to guess passwords. Dictionary attacks will find easy to guess passwords.
7. If logging on remotely to a system use ssh which encrypts username and passwords. Disable telnet if possible as this sends usernames and passwords in plain text.
8. Implement a firewall with a DMZ when connecting computers to the internet. If you have the resources to implement a web proxy do so. However web proxies do hinder user privacy, so you need to be clear about your value systems.
9. Install and regularly update anti-virus, anti-spyware and anti-spam software. It won't stop an unknown attack on your system, but it will protect you from a sucker punch.

10. Treat e-mail as an insecure if handy medium for sending messages and files.  
Never open files that you have not verified the origins of. This may take the form of phoning the sender and asking what's in the attachment or using PGP to encrypt messages from regular correspondents. If an application or attachment is to be kept secret use the regular post as there are serious legal repercussions for intercepting the Mail.
11. Beware of social engineering. People will masquerade as someone you know or trust and ask you for PINs, passwords. **Never** give out passwords or PINs unless legally obliged to do so.

For more information contact: [info@howesystems.com](mailto:info@howesystems.com)