

HOW MANY FORMER EMPLOYEES CAN ACCESS YOUR COMPANY'S NETWORK?



We're Local - Here To Serve You

- Information Security Strategy
- Network Management and Administration
- Certified Experience: CISSP | MCSE
- 13 Years in the Industry

Don't Turn Your Back on Local Network Security Management

**Minimize Risk While You Maximize Efficiency
Call Us—We Can Help You Today!**

Best Practices for Passwords

Passwords are everywhere and they're the frontline defense against unauthorized access to your network. A strong password is difficult to crack because of its complexity. Try the following best practices:

- Use a password of at least seven characters.
- Change your password maybe twice a year.
- Include upper and lower case characters.
- Include numbers between 0 and 9.
- Include symbols such as #, \$, or !.

A great way to remember complex passwords is to replace specific characters with a word you'll remember. Here's a complex example that's easy to remember: **g0Lph3r!**
Some don'ts with passwords:

- Never use your name, kids names, birth date, or SSN.
- Never use an open phrase, word, or name—computers can easily match passwords to dictionary words, terms, common names, and expressions.
- Never use the same password in untrusted spaces (like the Internet) that you do in trusted spaces (your company's network).
- Never write down passwords.
- Never share your password with anyone.

Studies show that as much as 80-percent of all IT crimes are conducted by internal and former employees.

So you think the problem is just external hackers? Think again.

Employees are usually given system access that circumvents traditional information security safeguards—they have insider information and capabilities. And without a proactive network security management plan, some of these permissions and capabilities are never turned off after employees leave the organization. That's one reason why more than 4 out of every 5 computer crimes take place *behind* your company's firewall!

What can you do about it?

1. Perform background checks on your employees.
2. Establish a working security and disaster recovery policy.
3. Perform routine audits to the policy to ensure compliance.
4. Allow the audits to become regular management metrics.
5. Use firewalls, strong passwords, anti-virus/spam tools.
6. Limit capabilities—only give employees the rights they need.
7. Setup automated security monitors to detect breach.
8. Have a good physical security plan.
9. Remove all sensitive company information from laptops or encrypt laptop contents to prevent compromise.
10. Seek an objective and professional opinion—think about managed services from local technology professionals.

**Hey—
We should call
these guys!**

**Mickler
& Associates**

More than great technology.

We install trust, respect, and value.

360.600.9508 | rmickler@micklerandassociates.com

www.micklerandassociates.com