

## **How to Strengthen Your Password or Why Your Password Could Be Your Company's Downfall**

At companies and frequently at home, user accounts may be protected by passwords. In many cases, you select the passwords so that they are easy to remember. They may be the same as your account name, they may be the word "password," or they may be the name of your pet. However, this is actually a very dangerous and risky scenario for you and can present legal implications for your company.

### **Why all the fuss?**

Even if you don't have anything of interest on your computer or in your mailbox, there are important issues to consider:

-> Do you really want others having the ability to send an e-mail under your name, which they could easily do if they had your password? A former employee or colleague whom you trusted at work could have a whole different mindset if terminated from a job.

-> Does your company run Outlook Web Access (OWA) or provide any other means of remote access? A weak, easy-to-guess password provides the first stepping-stone for a would-be hacker or mischief-maker to gain full access to your corporate data.

Let's discuss hackers for a moment. You might think "Why would anyone want to hack me? I have nothing important on my computer." However, the truth is that most hackers don't really care about your data. They want to gain access to your system so that they can then turn around and launch an attack against their true target. And if the attack is ever traced back to its origin, you or your company will be the party that's held responsible. Hackers are constantly probing your system for such opportunities, whether you're a Fortune 500 company, a small accounting firm, or a home user. And weak passwords are your biggest vulnerability.

MicroData Group, Inc. strongly encourages a solid password policy to aid in the prevention of any kind of unauthorized access, whether from other employees or from hackers. To select a "strong" password, we recommend the following guidelines:

1. Passwords are always case-sensitive
2. Passwords must be a minimum of 6 characters. The more characters that are included, the harder the password is to guess or crack
3. Passwords should not include your account name or any part of your real name
4. Passwords should contain a mix of alphanumeric characters and "special" or punctuation characters, such as "/\*\$"
5. Passwords should be changed periodically.
6. Passwords should not be recorded or stored in any location, such as on a sticky note or other PC.
7. Passwords are not to be divulged to any other person, including the network administrator. [The network administrator always has the ability to change a password if necessary for management purposes.]
8. No one should log on for anyone else.

Additional password guidelines:

1. Passwords should be made of more than one word (e.g. myrobot) as this prevents the use of "dictionary attacks" which utilize a standard dictionary as the basis for trying thousands of passwords.
2. Passwords should utilize mixed-case characters for extra security (e.g. mYroBOT) - this makes the guessing of them even harder
3. Insert numbers where characters would be found (e.g. mYr0b0t) or anywhere in the password (e.g. mYroBOT2)
4. Passwords should be easy to remember, but not easy to guess. "Passphrases" are acceptable to use if they are easier to remember than passwords. An example of a sufficiently complex passphrase is "myrobotIsMypassWord."
5. Do NOT use "myrobot" as a password