

Are your passwords secure?

practice

PRO

Protecting your passwords

It's one of those maxims that can't be repeated often enough: Treat your passwords as the confidential "keys" that they are. Much like the keys that open your front door or start your car, computer passwords are the keys that "unlock" your computer.

The following are some steps you can take to protect your passwords and keep your data secure:

- never write down your password, especially on your monitor. Is this not the same as leaving the keys for your car in the ignition? Take a walk around your office and see how many passwords you can find on monitors.
- if you absolutely have to write down some of your passwords to remember them, don't write them out exactly. Write them out so they have to be translated in some way. For example, add or delete a character, transpose letters, or vary them some other consistent way which only you can figure out.
- don't tell anyone your passwords. Change any compromised password immediately, even if you only *suspect* it has been compromised.
- don't use the same password for everything as you could be giving someone full and easy access to your entire system. Try to use different passwords for different programs, especially for your network logon password.
- on Windows 2000 and XP computers, don't have identical passwords for your network logon and administrator account passwords.
- ideally you should change your network password every 60 to 90 days.
- be careful about where you save your password on your computer. It is not uncommon for people to have a Word or WordPerfect file with all their passwords in it. This file can be easy to find, especially if it is called password.doc, or if it contains the word "password."
- be wary of dialog boxes, such as those for remote access and other telephone connections, that present an option to save or remember your password. **Do not select this option.**

Creating "strong" passwords

Passwords can be the weakest link in a computer security scheme. Strong passwords are important because password-cracking tools continue to improve and the computers used to crack passwords are more powerful. Network passwords that once took weeks to break can now be broken in hours.

Password cracking software uses one of three approaches: intelligent guessing, dictionary attacks, and automation that tries every possible combination of characters. Given enough time, the automated method can crack any password. However, it still can take months to crack a strong password.

For a password to be "strong" or harder to break, it should:

- be at least seven characters long;
- contain at least one character from each of the following four groups:
 - uppercase letters A, B, C, ...;
 - lowercase letters a, b, c, ...;
 - numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9; and
 - symbols (all characters not defined as letters or numerals, including: ` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : ; ' < > ? , . /
- have at least one symbol character in the second through sixth positions;
- be significantly different from any passwords you have used previously;
- not contain your name or your computer user name;
- not be a common word or name.

Treating passwords as confidential keys to your computer assures you and your staff secure your client's data.

