

5 tips for top-notch password security

Whether it's a few PCs or hundreds on your network, there's one thing that can separate your system from being compromised: a great password.

Why? Hackers want access to anything and everything. If they can guess your user name and password, you might as well have given them your wallet and the keys to your building.

Before we talk about what makes a good password, let's begin with the first of five things to know and practice in using passwords.

1. Don't be complacent: Attacks can and do happen.

Hackers are a devious bunch and will stop at nothing to get into your network and files. They use three different methods to get to you: brute force, dictionary attacks and social engineering.

Brute force is the most time-consuming method. Basically, it involves a program that tries every combination of letters, numbers and keyboard characters to guess your password. It starts with trying every character, then tries two-character combinations and so on.

The longer the password is, the exponentially more difficult it becomes to crack. According to George Shaffer, a password expert, a password that is eight characters in length and utilizes lower- and upper-case letters, numbers and keyboard characters won't be cracked for two years. This underscores the importance of being as random as possible when choosing your password. (More tips from Shaffer on creating passwords are available at www.geodsoft.com/howto/password).

Another method of attack is through the use of custom dictionaries. These dictionaries are filled with words and names, but also number and letter combinations, such as 11111 and abc123. Simple passwords such as "duke" or "ilovemydog" can easily be guessed.

The third and most effective method of attack is social engineering. This involves someone with criminal intent soliciting a password directly from a user. Many people divulge their passwords to co-workers and strangers without even realizing it.

For example, most small businesses don't have a dedicated information-technology staff. A hacker posing as someone from your company's Internet service provider could call in and get an unsuspecting employee's password by "testing the service." The hacker might request the employee's user name and password to log in and test the connection from the ISP's end. If the hacker sounds authoritative and legitimate enough, your whole network could be compromised.

If your business rents space in a larger facility, strangers probably roam the hallways unnoticed. A few innocent questions or a watchful eye can be disastrous.

2. Know what makes for a bad password.

Because the attacks described above are becoming increasingly more common, you don't want to use anything in your password that's personal and easy to guess. Keep in mind the following don'ts:

- Don't use only letters or only numbers.
- Don't use names of spouses, children, girlfriends/boyfriends or pets.
- Don't use phone numbers, Social Security numbers or birthdates.
- Don't use the same word as your log-in, or any variation of it.
- Don't use any word that can be found in the dictionary — even foreign words.
- Don't use passwords with double letters or numbers.

Some of the worst passwords are: password, drowssap, admin, 123456, and the name of your company or department. Finally, never leave it blank. That's a surefire way to let the bad guys into your system.

3. Get proficient at creating good passwords.

A good password is one that is easy to remember but difficult to guess. That sounds like a paradox, but it's really not.

There are a couple of different ways to create difficult-to-crack passwords. One is substituting letters with characters and numbers. To make it easier on yourself, try to use numbers and characters that resemble the letters they are replacing.

For example, you would never want to use the word "password" as your password. If you change it to p@7sw0rd!, you've got something that would take some time to crack but is fairly simple to remember.

Another method is to use the first letters of the words in a favorite line of poetry or a verse of song. "Hail, hail the lucky ones, I refer to those in love" becomes "H,hTL0,IR2t1L."

The best passwords are at least eight characters in length and use a combination of numbers, keyboard characters and upper- and lower-case letters. The longer your password is, the longer it will take someone (or more likely, some program) to crack it.

4. By all means, safeguard your password.

At first, it may be difficult to remember your password. Did you substitute an "i" with a "1" or did you use a "1" to represent "L?" Most people will want to write the password on a piece of paper and place it underneath their keyboard or mouse pad. Or worse, they'll stick the password right on their monitor.

To help remember the password, use it immediately. Then log in and out several times the first day. Just don't change it on a Friday or right before leaving for vacation. You could write it out

several times on a piece of paper. This helps record it in your mind. Just be sure to shred the paper when done.

Invariably, there may come a time when a password has to be shared. Let's say an employee is out of town to give a presentation but left the PowerPoint file on his desktop. You will have to get his user name and password to access that file. After you open the file, change the password and give him the new password upon his return. Then, as soon as the person gets back into the office, have him change the password again. Yes, it's a lot of work but well worth it.

5. Change your password often — as in several times a year.

Your network administrator can force your employees to change their password every so often. By default, passwords are set to expire every 42 days in Windows Server 2003. Microsoft recommends having users change their passwords every 30 to 90 days, but encourages you to go with the smaller number. I think 30 days is a reasonable number here. You always want to side with caution when it comes to sensitive information.

If you're like me, you allow your employees to do light surfing at lunch and on breaks. Encourage your employees to change their passwords to personal Web sites as well — such as to banking, Internet e-mail accounts, shopping sites, and so on. Advise them not to use the same password for all of their sites. A particularly good hacker can cause personal financial ruin by gaining access to one username and password.

Now the following is an eerie thought — but it's something that must be taken into consideration.

What if you or your network administrator dies?

Well, if you've used best practices when creating a password, nobody else knows your password. And it's so complex that it could take months to crack the code or money to buy the right software for the job. Just in case, you might consider keeping a copy of all passwords in the company's safe. As for your personal passwords, keep them stowed away somewhere along with your will.