

Password Strategy

by Gary A. Campbell, gacWebSolutions

On the old mainframes and minicomputers, passwords were used to keep Ralph, the guy in the next cubicle, from messing with your files. Back then your six digit birth date was enough to secure your files. Today's threat is far more sophisticated than Ralph. Hackers now employ high speed password generators to discover your passwords. And as our computers have evolved so has the data we store on them. Once a hacker cracks your password, he can access your email, bank accounts, health records, buying habits, and more. Our passwords, being the first line of defense, have to evolve as well.

The bad guys boast that there isn't a password they can't hack one way or another. Security experts agree. With the technology available to hackers, it is theoretically impossible to create a passwords that is 100% secure. Our objective has to be to select a password that is impractical to crack because of the computing power and time required. Hackers will turn to easier targets*.

With this in mind, what makes for an effective password? The most secure passwords are very long strings of completely random, patternless characters. But they aren't practical because they are not memorable. So here are some practical guidelines:

- Some hacking tools start by running through dictionary entries, both English and foreign, looking for a match. Avoiding names and dictionary words will protect your password from these "dictionary attacks".
- It must be easy to remember. Think of a sentence or phrase that is personal to you and use it as a starting point. Maybe something like, "I first ate sugar cane at Trader Joe's". Next, take the first letter of each word to create a new word. In our example, that would be 'IFASCATJ'.
- When it comes to the number of characters, more is better. A password consisting of eight capital letters presents 208 trillion possible combinations (26 possible letters raised to the 8th power). As of this writing a hacker employing a brute force approach on a single computer can run through 500,000 possible passwords per second. At this speed he could test every possible combination in about 115 hours. We can increase the complexity considerably by including lowercase letters, numbers and typographical symbols. Now our sample password might be 'i18\$c@Tj'.
- Until you get the hang of creating secure passwords, you might consider testing the complexity of your new password. There are many websites out there offering to test it for you. While most of these sites may be legitimate, don't you think that'd be a great way to gather passwords? If you trust Microsoft, click [here](#) to use their password checker.
- Employ multiple passwords to diversify your exposure to risk. If a password is compromised, assume all the data protected by that password is compromised. This doesn't mean you have to memorize dozens of passwords. All you need to do is add one or two descriptive letters to the front or back of your strong password. For example, your eBay password might be 'i18\$c@TjEb' or 'eBi18\$c@Tj'.
- Because some intruders can go undetected for long periods of time, you should change your password at least every 90 days.
- This may seem obvious, but once you settle on a secure password, KEEP IT SECURE! If you must write it down somewhere, write it lightly on some memorable page in a memorable book on your shelf (but don't label it 'Password'). Because your password is the key to all your data, don't hide your password anywhere you wouldn't hide your data.
- Never include your password in an e-mail as email is easily intercepted.

- Internet fraud is rampant. Never respond to an email request for your password. Never respond to an email that asks you to go to a website to verify your password. Internet "phishing" scams use fraudulent e-mail messages like these to obtain passwords.
- And finally, don't ever type your passwords on computers that you do not control, especially public computers. You never know who may have loaded a keystroke logger onto the machine.

* *This is analogous to the story of two campers who hear a grizzly bear outside their tent. One camper calmly starts to put on his running shoes. The other camper says, "What do you think you're doing? You can't outrun a grizzly!" The first camper replies, "I don't have to outrun the grizzly. I only have to outrun YOU!"*

© 2006 gacWebSolutions
contact: gary@gacwebsolutions.net