The Key to Choosing a Good Password

Easy to Remember-Yet Hard to Guess

By John J. Wills

Choosing a “good” password is very important to the security of any system, particularly systems where confidential information is at stake. But what constitutes a good password? Is it one that’s easy to remember? Or one that’s hard to guess?

Let’s look at the two extremes. What are the easiest things for you to remember? For most people, the list includes their own name, a spouse or child’s name, the name of a pet, or a birth date. This list also happens to be the same list hackers or others will use in trying to guess your password. The better the guesser knows you, the more likely they are to know your spouse or pet’s name. So, as a general rule, these are bad choices for passwords.

What about a password that nobody is likely to guess ? like GI2C4O? That would be a great password if you had a way to remember it. But, if you’re like most people, you would have a hard time trying to remember such a password so you’ll have to write it down. Any password that is written down is not a good password because someone may find where you’ve written it.

The key is to balance “easy to remember” with “hard to guess.” First, let’s discuss some ways of selecting passwords that are hard to guess. One proven method is to make your password at least seven characters long. If your password is only one character long, it would take no more than 40 guesses to figure it out (assuming letters A-Z, numbers 0-9, and the symbols $, @, #, _ are the only valid characters). Add a second character and there are now 1600 possible combinations. With seven characters there are 163,840,000,000 possibilities. That’s a lot. Even password guessing programs will take a while to figure out a password with seven or more characters. That number gets even higher if your system differentiates between upper- and lower-case letters.

Notice that numbers and symbols were included in the list of available characters. Check with your Network Administrator to find out what choices are available on your network. And then use them. For one thing, if you limit yourself to only letters, even with seven letters, you’re down to only a measly 803,181,0176 possible combinations. But seriously, easily guessed passwords become much harder when a number or symbol is stuck at the middle or end. Even if everyone knows your dog’s name is Sparky and you got married in 1972, who’s likely to guess your password is SPARKY72?

That example also illustrates another method?combining two unrelated (or seemingly unrelated) items. Cooking ingredients and clocks may not seem to have much in common but you probably wouldn’t have much trouble remembering THYMECLOCK as a password.

What about the convoluted example above – GI2C4O? Do you think you could remember that? Maybe you could associate it with a phrase you’re likely to remember such as “(G)arfield (I)s too(2) (C)ool for(4) (O)die.” Even if the phrase you come up with is nonsense, it’s likely to stick in your head better than a random string of letters and numbers.

Of course, it doesn’t matter how good your password is once it’s been compromised – whether someone took the time to try every combination, watched over your shoulder while you typed it in, or whatever. Once your password is in the wrong hands, a devious person will have free rein of your computer and/or the entire system or network. It is important to change your password any time you think it may have been compromised. It is also important to change your password on a regular basis as it may have been compromised without your knowledge.

How often should you change your password? That depends largely on the size of the system or network as well as the type of information contained on it. And remember, if your network is connected to the Internet, your network is now worldwide. Within a typical company with a well-protected firewall and fairly controlled work environments, changing your password every three months or so is probably a good idea. If you have more system privileges than the typical user you should consider changing your password more frequently.

How do you come up with an easy to remember yet hard to guess password every 90 days?

If you follow the advice above, you will use a number in your password. Why not make that number represent the month in which you set your password? Or, better yet, the month in which you will have to pick your next password. That way, every morning when you log in, you will be reminded of how long you have left to come up with a new password.

But don't just use the same password with a different number. That lessens the effectiveness of your password back down to only 10 or 100 combinations. I once had a roommate who broke into my locked briefcase because he was bored. He tried 000, then 001, etc. until the lock opened. The possibility of taking up to 1000 attempts didn't deter him. Having 163,840,000,000 possible choices probably would have.

You could also use the month idea with words. Think of something the month reminds you of – a flower, a food, a color – anything that you are likely to remember. For example, say you need to pick a password that you will need to change again in July. Maybe July makes you think of 4th of July cookouts. Set your password to HOT7DOG. July is the seventh month and you eat hotdogs at cookouts. Okay, for you vegetarians out there, how about CORN7COB?

In summary, if you follow some or all of the following suggestions, you'll have a password that contributes to a secure network and that's easy to remember?yet hard to guess.

- Don't choose "obvious" passwords such as your spouse, child, or pet's name.
- Don't choose a password that's so hard to remember that you have to write it down.
- Choose a password at least seven characters long.
- Choose a password with at least one number and/or a symbol in it.
- Combine two unrelated words to form a password.
- Use associations to remember your password.
- Change your password on a regular basis.
- Change your password whenever you think it may have been compromised.
- Never reuse any password.
- Never use any sample password used in this article or any other guide.
- And, most importantly, never give your password out to anyone.