What’s a good password?

System and security administrators often have to explain to naïve users that “Betty4me”, “myDog*Bowser” and “password6” are not good passwords. They are too easy to construct using dictionary-based attacks <http://www.tech-faq.com/dictionary-attack.shtml> that compare one-way hashes of combinations of real words mixed with numbers and symbols with the one-way hashes of user passwords stored in password files. Some of them are also too easy to guess if the attacker knows something about the private life or preferences of the user (like the name of the user’s dog).

Some helpdesks suggest to their users that they try public password generators. I looked at a few and have the following comments on what I observed.

For purposes of comparison, I limited my search of passwords to 10 characters which had to include letters, did not use mixed case, included numbers, and included punctuation. I kept mixed-case out of the passwords because I think that remembering which letter is uppercase or lowercase in a more-or-less random string increases the difficulty of remembering the password and therefore the likelihood that a user will write it down. Where possible, I generated 10 suggested passwords at once.

My first test used PC Tools Software’s “Secure Password Generator.”<http://www.pctools.com/guides/password/> The Web page allows selection of length, use letters, mixed-case, number, and symbols and also allows the user to exclude similar-looking characters (l, 1, I and o or 0). Here’s a sample pass with 10 characters, lowercase only, including special characters and excluding the confusing characters:

```
drud8?a*et
=r8st8t7ud
!78et9cr*
4e@ufrugac
8_sececeu
gath65*ke*
9#upura_r!
$estugethi!
*e_uka&ra3
6etr=xuspa
```

Hmm, I’m not sure that these are particularly easy to remember, although at least there seem to be nice alternations of one or more consonants with a vowel, making it possible to try pronouncing them. However, I think that the unconstrained gibberish is worse:
Yechhh! This alphabetic farrago is asking for calls the HelpDesk for password resets – or sticky notes on the underside of the keyboard.

More next time.

* * *


* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.