I have long argued that passwords are a terrible way of authenticating identity:

- Many well-meaning but unaware people choose really stupid, easy-to-guess passwords such as the names of people important to them (or favorite sports teams, or the product whose billboard is visible from their office window, or the names of objects on their desk);
- Good passwords increase the keyspace not only by being longer but also by using upper- and lowercase letters, numbers and special characters – resulting in monstrosities such as “j3q(K8bX_*5” – and let’s not even _think_ about allowing “O” and “0” in the character set;
- Some users generate their passwords using funny rules such as using particular letters from the words in phrases (e.g., using the third letter of each word in “Mary had a little lamb; its fleece was white as snow” produces “rdatmsesiso”) – and then they forget the rules;
- People sometimes use numerical increments to get around rules preventing password reuse (e.g., fisu3nema, fisu4nema, fisu5nema . . .) thus compromising their _next_ password as soon as the _current_ password is discovered;
- Users often use exactly the same password for everything (their private Web e-mail, their corporate professional e-mail, their DVD-club login, their talking-slug club – everything) with the result that any single password compromise is a potentially complete security compromise;
- Making passwords hard to guess forces many people to write them down;
- Physically-recorded passwords get stored in the same places network security auditors have always found them: in desk drawers, under keyboards, under chair seats, in files labeled “C:\passwords.txt” and even in plain view on the back (or front!) of video screens;
- When people _do_ pick hard-to-guess passwords and _don’t_ write them down, they often call the HelpDesk or security administrator to reset them because they _forget_ them, causing a great deal of irritation and wasted time for everyone concerned.

A study <http://www.nucleusresearch.com/press_releases/prpassword1006> published last year by Nucleus Research reported findings on user behavior concerning passwords. To no one’s surprise, the researchers found that “More than a third of employees write down or electronically record their passwords, creating significant vulnerabilities. Even worse, lowering the quantity of passwords, changing password complexity, or changing password change frequency had no impact on employee actions.” They also found that “There was also no correlation between complexity, frequency, and quantity and how often users called the help desk with password-related issues. Seventy percent of enterprise users call the IT help desk once a year for help with a forgotten or missing password; 16 percent call two to three times a year; 9 percent call three to five times a year; and 5 percent call more than five times a year for password help.”

The full report is usually available by subscription only, but the company has very kindly opened it temporarily for use by readers of this column <http://www.nucleusresearch.com/research/g68.pdf>.
> Based on a survey with 325 respondents, efforts at improving password management by ordinary users generally fail. Specifically, the same proportion (1/3) of users keep a written record of their password regardless of the amount of
- user education,
- password complexity,
- security-policy restrictiveness.

In my next column, I'll look at how these findings relate to what cognitive psychologists know about our capacity to understand risk.

Nucleus Research is an IT-related research organization that takes a unique investigative approach to its research and helps end-user organizations assess the value realized from technology acquisitions. To learn more, please visit www.NucleusResearch.com. My thanks to the company for opening their proprietary research report to readers. [I have no financial relationship whatever with Nucleus Research.]

* * *

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.