©2007 Hospitality Upgrade
No reproduction or distribution without permission.
For permissions, high quality PDF or reprint fees
contact info@hospitalityupgrade.com.

By Michael Schubach

# On Beyond Open Sesame
# Are We Safe Yet?


©iStockphoto.com

I've become obsessed with security. In the last issue of *Hospitality Upgrade*, I wrote about the dangers that beset hapless users who execute financial transactions on unmonitored public-access machines. By addressing the traveling public, I thought I had the target demographic pretty well nailed. However, there were a number of readers who noted that while the article was "interesting yet alarmist in nature," it failed to resonate with the true core readership: the shut-ins. You know, those folks who conduct their visits to cyberspace from the safety of their own little desk or cubicle. They sit in their hermetically sealed network bubble, knowing that they have a terrific IT staff to back them, a wonderful firewall to protect them, and great anti-everything software to keep them safe when they venture into unfriendly cyberterritory. Their motto is drawn from the immortal words of *MAD Magazine's* Alfred E. Neuman, "What, Me Worry?"

view online
Please see a reader's response to Michael's previous article, "A Farewell to Arms." The response elaborates on opportunities and safeguards for public use computers, and is found on ***pg 179*** of this issue.

The unconsidered element that everyone seems to brush by is the step zero of system security – the guardian at the gate that prevents unwelcome guests from gaining access to the bubble in the first place. No, not the bouncer; I am referring to the password. Moreover, I reference not just the plain old password but the secure password, one that actually provides adequate protection.

For that portion of the readership that is unfamiliar with computer applications and therefore has no real business reading a technology magazine, let me answer the basic question that must be driving you crazy as you wait to see your doctor: what makes a password really secure? Believe it or not, a lawyer defined the term in a service agreement I reviewed recently. According to this highly informed source (assuming that his hourly rate accurately reflects his level of expertise), secure passwords are "between six and eight characters long, contain letters of mixed case and non-letter characters, and cannot be found, in whole or part, in normal or reverse order, in any dictionary of words or names in any language. The [user] is responsible for changing his or her password regularly."

Now that the American Bar Association has been kind enough to weigh in on the matter, let's figure out the ramifications of the fine print. We will begin our search by exploring the basic design concept of the password. In documented use since ancient times, passwords were designed to serve an obvious but important purpose: the ability to recognize a stranger as friend or foe. To that end, the password should be sufficiently challenging that foes can't guess it but sufficiently easy that friends will remember it. This baseline requirement for simple complexity leads us to the most notable problem with passwords: most users today don't have the memory capacity required to avoid being a serious threat to their own organizations.

Knowing that the safety and security of the bubble are at stake, we ask users to create unique passwords for network access, e-mail access and application access for one, two or three applications depending on job function. Beyond those applications are the ubiquitous timekeeping and expense reporting modules, as well as insurance or benefits programs. Of course, these passwords are in addition to the user's personal e-mail, ATM PIN number, telephone calling card code, online banking service password, copy machines and the access codes for any other subscription-based services they run. Wikipedia cites NTA Monitor, a prominent Internet security company based in the United Kingdom, as the source of an interesting statistic: the typical intensive computer user maintains 21 accounts that require a password. (This is a considerably higher total than was required in the days of the Roman Empire.)

> The typical intensive computer user maintains 21 accounts that require a password.
> *Source: NTA Monitor*

If your organization takes network security seriously, then you or your IT professional will issue those easy-to-use secure password requirements endorsed by the ABA: 6ix to ei8ht letters and n0n-letter$, rand()mly miXiNg caSes in such a fashion that the result cannot be found in any word or name dictionary in any language, either forwards or backwards. Then, if you're really serious, you'll ask those users to change those passwords regularly, being careful not to repeat any of their previous selections.

The interval you choose for tumbling passwords demonstrates your true level of seriousness. You can send your users through re-authentication once a month, quarter or year. Regardless of the schedule you pick, there is one more tiny detail the users must observe: they must never write down any of this year's 21, 84 or 252 unique choices anywhere.

It's no wonder we've had to invent a new disease to describe the feeling of hopelessness that the average computer user feels when he or she tries to remember his or her security data: password fatigue. (See, it's a good thing you're at the doctor's office.) With the introduction of our third IT-centric disease (after carpal tunnel syndrome and fried eyes), we may have finally come down to the basic issue that plagues network administrators everywhere: are we our own worst enemy?

**It's no wonder we've had to invent a new disease to describe the feeling of hopelessness that the average computer user feels when he or she tries to remember his or her security data: password fatigue.**

If we are to be good network custodians without driving our users to the brink of fatigue or insanity, we should consider the following:

1 **Keep security requirements in perspective.** Easier typed than accomplished, but we really need to review security policies so that they are proportionate, sound and reasonable. On the one hand, as guests visit our establishments and Web sites, we might remind ourselves that we typically do not deal with life-and-death issues or pressing matters of national security. On the other hand, between our personnel, financial and guest service systems, we store a tremendous amount of sensitive data that could present an embarrassing (or potentially devastating) liability if that information is compromised. You may just come to the realization that big-system security is something your organization genuinely requires.

2 **Remember that there are alternatives to password security.** With each passing day changes are being made to the security landscape. We now have biometric options, security devices that issue one-time entry codes (electronic key fobs that tumble your password every 30 seconds) and graphics-based systems that allow users to remember faces or pictures instead of letter sequences. We're beginning to see phones and PDAs that provide encrypted password storage documents so that you can store your passwords in an off-network device that only you can access (if you remember your password and your phone or PDA isn't stolen). Finally, there is the option of single sign-on technology. The good news is there's not much to remember or forget. The bad news? See if you can guess… and if you do, you're into everything.

3 **Don't impose a standard so high that you end up with no standard at all.** Best intentions often produce the worst results. If you insist on uncrackable complexity and strict observance of the Big Two Laws of Never (never write it down and never use the same password for more than one application) then you're likely to guarantee that your network friends won't be able to get themselves admitted to the bubble. When that happens, users will circumvent the rules to escape fatigue and to make their lives operable. That turn of events really puts your network at risk. Your cyber foes become a more realistic danger than they were in the first place because now there is no reliable security standard in effect.

What to do? System security issues can feel like a tempest in a teapot – a lot of hypothetical discussion about a threat that seems never to materialize. Besides, IT professionals fear the outbreak of a fourth IT disease: manager fatigue (also known as the "shut up and get out" syndrome). However, the threat can be real and the enemy's arsenal is substantial. Readily available dictionary-based attacks (programs that simply throw every known word including letter-symbol repl@cements at a target application) can do so at a rate of more than 120,000 attempts per second, well over seven million attempts per minute. (That rate has also gone up since Caligula's day.)

**Reinforce to the folks in the bubble that the issues are genuine, lapses can be catastrophic, and that their attentive assistance is appreciated.**

The most reasonable outcome occurs when you keep the security issue in front of your users. Statistics indicate that the more time and attention that you give network users on the issue of security, the better the job they do in maintaining standards. Trained employees make better password choices and keep them more confidential than untrained employees. Suggest using acronyms instead of words as a memory aid; an acronym is easier to enter and harder to crack (E2EAH2C). Network supervisors can purchase one of the better-known password cracking programs to check the strength of passwords in use on your systems today and help those users who can't help themselves. Reinforce to the folks in the bubble that the issues are genuine, lapses can be catastrophic, and that their attentive assistance is appreciated. And remember that, in the immortal words of Tarzan, "It's a jungle out there."

*Michael Schubach is vice president, information technology, for Pinehurst Resort. Located in the Village of Pinehurst, N.C., Pinehurst has just been named the site of the 2014 U.S. Open golf championship. You may e-mail michael.schubach@pinehurst.com and he will respond provided he can remember his e-mail password once he remembers his network password.*