Coping with Strong Passwords

By Charisse M. Sebastian, CNE

[M. E. Kabay comments: I was invited to speak at a meeting of the New England Information Security Group <http://www.neisug.com/> in May 2004 and was delighted to meet Charisse Sebastian. We had such a great time exchanging stories and ideas about technical support and security that I invited her to write about her insights into the importance of good communications between the IT group and the user community. Here is her contribution to the column with my thanks.]

***

In previous articles about passwords, Dr Kabay has expressed his distaste for this method of identification and authentication (I&A). But whether he likes them or not, most of us are stuck with passwords and the management problems they cause.

In an age of hackers, viruses, terrorism and malevolent employees, talking about security can make people either try to glamorize it, à la James Bond, or minimize it, as in, “It won’t happen to me.” Both attitudes are distractions that decrease security. Security is too often an afterthought, especially in the United States, where the American culture of openness can interfere with effective security. Openness is a valid and altruistic attitude for social interactions, but protecting networks from intrusion and accidents is crucial to long-term success in business. Unfortunately, efforts to make users more aware of security are often met with the attitude that IT must be paranoid or with silent resistance.

The most common sources of conflict where IT and users interact over security are password-protected logins and Internet communications. Until we see affordable improvements in I&A, strong passwords and good management remain essential.

In today’s environment, everybody connected to the Internet is a potential target.

Some salient statistics – for what they’re worth:

* Calls dealing with password resets are the #1 demand for help desk support. [1]


* Percentage of U.S. companies not implementing “adequate” security: 30% [3]

* Percentage of U.S. companies that spend 5% or less of their IT budget on security for their networks: 50%. [4]

Strong passwords require 8-14 characters, minimum and a mix of case, numbers and symbols. But to a user, strong means more complicated. Users either simplify the password itself or help themselves remember it -- often with a Post-It (TM) note on the monitor bezel or under the mouse pad.
This issue requires human interaction to resolve. First, I cannot emphasize enough the importance for IT staff from the CIO on down to the lowliest help desk assistant to avoid condescending to users – as in, “We’re IT and they’re just users.” Learn what the users are thinking. How do they view security? Why and how have they opposed security? Instead of dictating to users from IT, look at the issues from the users’ point of view. Get them to buy into the policy willingly and enthusiastically as stakeholders, not as put-upon victims of an administrative dictatorship. As a suggestion, as part of new employee orientation (and an existing employee refresher too), have the IT instructor go to a criminal-hacker Web site to show users the kinds of threats that IT has to deal with every day and how such threats can harm the users directly and personally.

Second, help users to incorporate strong passwords in a way they can remember them, without writing them down. Suggestion; run together words in common phrases up to about 16 characters, mixing case and substituting/adding symbols and numbers for some letters.

Third, with user input, create a well-defined, solid foundation of company-wide policies and procedures. That means for everyone from the CEO on down, no exceptions. For end users to become stakeholders it’s critical that they understand that everyone is involved and why. Why does IT need their help? Why do they need to be concerned? Why are IT in effect an extension of their own departments?

In summary, computer security is an endless process. With continuing user investment and input in a real team effort with IT, security becomes manageable, effective and non-intrusive. Often, instead of purchasing some new piece of security technology, getting users actively involved in security could save further strain on already tight IT budgets. The process of finding or creating the mix of technology, procedure and policy involves analyzing the system including input from users to understand what is needed. Once new procedures are in place and policies established, they have to be maintained, monitored and tested on a regular basis. That includes feedback from the users, taken seriously, on a regular basis.

Computer security is a journey, not a destination.

***

References

[1] Courion Corp Password Management Overview


***

Charisses Michelle Sebastian (mailto:char-sebastian@att.net) is an IT Support Evangelist and passionately loves IT, specializing in desktop/user support, troubleshooting, training, server
support, security, writing and mentoring. Right now, while working in a consulting practice and in transition, she is on an active job search and invites correspondence.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 Charisse Michelle Sebastian. 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.