MIT MANAGEMENT SLOAN SCHOOL

Cybersecurity at MIT Sloan

Do you Have Password Headaches?
You are Not Alone, and it is Unnecessary!

Stuart Madnick

Working Paper CISL# 2020-14

March 2020

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Do you Have Password Headaches?
You are Not Alone, and it is Unnecessary!

Stuart Madnick (@smadnick2) is the John Norris Maguire Professor of Information Technologies at the MIT Sloan School of Management and the founding director of the Cybersecurity at MIT Sloan (CAMS) research consortium. *Acknowledgement*:
This research was supported, in part, by funds from the members of the CAMS**.**

At least once a year—but every two or three months in many offices, the Better Business Bureau even recommended changing very month—we all receive the corporate email telling us our network passwords are expiring and it's time to create a new one.

The logic is straightforward. If a hacker happens to discover your password, the amount of time during which he or she can do damage is limited. In addition, frequently changing your password may make it less likely somebody will guess it.

But none of this matches reality. For starters, if a hacker discovers your password, they don't wait months, weeks, days or even hours to take advantage of it. They quickly move through the organization—both laterally and vertically—rapidly harvesting many more passwords along the way. So changing passwords once a year, once a month, even every few days is too late to prevent serious damage.

In fact, forcing employees to constantly change their passwords does the opposite of what is intended: It makes a corporate security system less secure, not more--not to mention the frustration employees feel and the productivity lost as they try to remember their new passwords.

What's more, the more frequently we are forced to change passwords, the more likely we'll use a password that a hacker can easily discover. That's because employees have so many passwords to remember that they often write them down, sometimes taped to their monitors, visible to visitors—and yes, this actually happens, even in security organizations—or make them as simple and easy to remember (and guess) as possible.

Researchers at the University of North Carolina studied whether password expiration met its intended purpose--"namely revoking access to an account by an attacker who has captured the account's password." The analysis of data from an organization that had practiced such frequent password change policies, led the authors to conclude "our study casts doubt on the utility of forced password expiration."

They found that, when faced with the need to change passwords frequently but to keep them memorable, workers commonly chose to enumerate their passwords. That is, "mypassword1" would be changed to "mypassword2." Thus, if a hacker discovered the old password, it was not hard to guess the new password. The researchers developed algorithms to automatically do the guessing and measured how easy it was. Their algorithm cracked 17% of the accounts in fewer than five attempts. And 41% of the changed passwords were cracked within three seconds.

Based on this study, the former chief technologist of the Federal Trade Commission concluded that "frequent password changes are the enemy of security."

Another study from Carleton University also demonstrated that frequent password changes hamper attackers only minimally and probably not enough to offset the inconvenience to end users.

This is not just a conclusion among academics. Key organizations including the U.K government agency Communications-Electronics Security Group and the National Institute of Standards and Technology (NIST) in the U.S. also concluded that mandated password changes are often ineffective or counterproductive. NIST published "Digital Identity Guidelines," which recommended decreasing both password complexity and the volume of forced password changes.

Obviously, given the increasing frequency and intensity of attacks, increasing cybersecurity is an important goal for every organization and every employee. But we need to carefully examine the impact of recommended security measures, and be sure that the benefits indeed exceed the costs. And employers need to remember one of the costs is the headaches that such policies inflict on employees. Maybe they will find they aren't worth those headaches after all.