federation forum
Spring 2010

Security Watch

Passwords – A Common Sense Approach

As countless people were stranded throughout the world thanks to the volcanic ash floating miles above Europe, companies and organizations alike may have been feeling the strain of operating without some of their key personnel for an extra-long, unplanned period of time. Most organizations' security and business continuity plans are structured such that mission-critical information continues to be accessible even with an extended absence of a key employee.

But in some, the only way that the "show can go on" is if the missing employee is electronically impersonated by someone who is in the office. The way to do this (according to many security best practices) short of assigning another user the same privileges in each system is to change the missing employee's password and allow someone who is able to report to work to login as that person to access the information. What typically happens though is that the employee who is unable to report to work will give their password to a coworker over the phone or via email so that their coworker can take care of their tasks while they are out.

We all know that sharing passwords is not highly regarded from a security standpoint, but occasionally "you've got to do what you've got to do!" The biggest problem typically encountered when this situation plays out is that the person receiving the password ends up writing it down. In even the best cases, that piece of paper inevitably sits near a computer where it can be used by anyone who is able to gain physical access to the building (janitors, visitors, etc).

If you do find yourself in this type of situation, you might give thought to asking the person to log-in using your password while you are on the phone with them and then ask them to immediately change it to a password that they know and will remember without needing to write it down. Given the number of their own passwords that person needs to remember, if they don't write it down and only use it once, they are far less likely to remember it. It would be wise for you to avoid leaving the password on a voicemail message if you can avoid it.

We each have tens or even hundreds of passwords that we need to maintain. So here are a couple secure ways to do that:

1. Instead of words, select phrases that are meaningful to you. A phrase will almost always meet the minimum length requirements and very few places have a maximum length requirement for passwords.
2. Develop your own system of password selection and maintenance. Why wait until you're asked to change your password or create a stronger password? With the focus on security, many organizations and systems are moving towards stronger passwords and asking you to change them more often. So pick your own system of selecting passwords and then change them on your own terms.

Passwords are intended to prove to the computer that you are who you say you are. Everyone knows how cumbersome passwords are to maintain and the industry has been developing various potential alternatives to passwords. It may not be too long before we are able to use various biometrics to authenticate our identity. Until then, we all need to do what needs to be done to make sure our world is secure.