Security 101: Password Management

By: Jim Mottola

Director oforensic Investigations
Risk Mitigation Services, Sobel & Co.

The first time many of us heard the magical phrase "Open Sesame" may have been on Saturday morning during the Bugs Bunny cartoon Ali Baba Bunny. The phrase was used by a character in order to open up a cave full of treasure, or so he thought. Once inside, he found a quixotic rabbit in the bottle. Since this passphrase was written in the early 1800s as part of the literary work, *Ali Baba and the Forty Thieves* it has been commonly known. Actually, in 2013 it was uttered by an actor to open the trunk of a Ford Escape. It would seem that passwords, PINs and secret codes are now ubiquitous in our everyday life and protecting them has become increasingly more difficult and important.

The Verizon Data Breach Report, the industry standard for recording trends in cyber-crime has often indicated that weak and stolen passwords are a significant risk to information security. Moreover, stolen credentials, which include both name and password, are both harvested by fraudsters during phishing attacks against users through spam e-mails and social engineering. These credentials are most often employed by criminals to log into web applications of financial institutions in order to commit fraud. And for small businesses, there have been numerous reports of targeted attacks or spear phishing of the log-on credentials of a company's commercial bank accounts in order to cause the fraudulent transfer of funds.

With so many ways to steal passwords to circumvent data security, what can business do to protect themselves? Moreover, what policies and standards will encourage employees to buy into to information security, through a practical approach?

1. **Setting the Standard:** Informing employees about the importance of these digital keys goes hand in hand with securing access cards and any other device used to enter your office.
2. **Know Where You Stand:** By identifying your key assets, you will be able to figure out what is your most important information. There are plenty of commercially available solutions from Apple, Microsoft and Google for data management and protection. However, I would encourage you to seek the consultation of an Information Security professional. Although there is no rule of thumb, I am going to state the obvious, get an opinion from someone you trust. I would look to a local chamber of commerce if you need a recommendation; reputations have a way of establishing credibility.

3. **Have a Conversation:** In either case above, you will need to establish a policy for password creation, retention and expiration. If using a professional, you should institute policies that fit your organization; remember your data and these conversations are vital to your business.
4. **Passwords are Not Rocket Science (Yet):** User names and Passwords, without an additional verifiable piece of identification make it difficult to know the true identity of the individual and thus make them vulnerable to compromise. In an enterprise environment, for most mid-size businesses and corporations more technologically advanced solutions are available such as Smart Cards, Fingerprint Scanners and Trusted Platform Modules (TPM). Like I said, almost Rocket Science. But here is the hard truth, no matter how sophisticated the technology, if you give someone your password, or they steal it as a result of failure to comply with basic security principals, they can be compromised. As in most cases, the above technology makes it harder, but not impossible, which leads us right back to where we started: Password Management.
5. **Password Construction:** Consensus among security experts holds that the most secure passwords, those which are hardest to guess or crack are determined by length, complexity and unpredictability. Therefore constructing passwords with a combination of upper and lower case letters, numbers and special characters, which are at least eight characters long is preferable. The problem for users is creating a password that is complicated enough to be secure, while being not too difficult to remember. By following this protocol you should have created a pretty tough password for someone to guess. Avoid using a variation of your email address, username or something out there in the public domain, like your cat's name or favorite sports team.
6. **Password Safeguarding:** Now that you have created a password, please do not write it down on a piece a post it, stick it on the bottom of your keyboard, desk or monitor. Or just as troubling, storing passwords, in a Word document or clear text, on any devise you own. Also, you should never give it or any personal information to a caller over the phone. If there is a security question or curious inquiry via email, beware. Pick up the phone and contact the requested party from a previously known or verified number. Furthermore, do not share your password with anyone unless they are a trusted and authorized internal Information Technology professional. And here is my favorite, do not walk away from your work station, without logging off, unless you want your boss to receive an inappropriate email sent in jest from a coworker or worse. That being said, as a business owner, having multiple passwords for various systems can also prove to be difficult for employees. Likewise, having one password for all access by each employee is also challenging. Most importantly, do not allow users to share passwords: each user should have a unique username and password for each system he or she is authorized to use, it creates their own user trail, which can be important, when things go wrong. If necessary, when many passwords are required, secure them in a locked draw, cabinet or on your person. Although, this runs contrary to some security professional's opinions, we need to be realistic or employees will just circumvent policies for practicality.

7. **Password Expiration:** The life of a password should follow the employment period of the employee. That being said, at the beginning or on-boarding, a password is created and when he/she leaves the organization, it should be retired. In between, it should be updated on a regularly established lifecycle, monthly, quarterly, bi-annually or annually, depending on your overall security posture and the assets you are trying to protect. The more assets: the more risk to your business, the more pro-active your security practices should be.
8. **Additional Guidance:** The National Institute of Standards and Technology (NIST) has established computer security recommendations and a Guide to Password Management. This guide from the US Government is a reasonable approach that takes into account the practical implementation of password management. Another source of guidance is Norton or Symantec and their many postings regarding cyber security and passwords.

Remember choose your passwords wisely, although sticks and stone can break your bones, poor password management can hurt you too. That's all folks…