Creating Secure Passwords

While we may find them annoying, and even take them for granted, it is important to remember why passwords are important: passwords are often the first (and possibly only) defense against intrusion (MacGregor). They protect personal information – information we don't want anyone and everyone to know. In our personal lives, this means financial information, health data, and private documents. In a professional context, this may encompass anything considered crucial to the success of the organization: trade secrets, financial data, intellectual property, customer lists, etc.

- Passwords can be cracked in a variety of different ways. The simplest is the use of a word list or dictionary program to break the password by brute force. "Brute force" software can make as many as 8 million password guesses a second!
- Another easy way for potential intruders to nab passwords is through social engineering: physically nabbing the password off a Post-It from under someone's keyboard or through imitating an IT engineer and asking over the phone.
- Many users create passwords that can be guessed by learning a minimal amount of information about the person whose password is being sought.
- A more technical way of learning passwords is through sniffers, which look at the raw data transmitted across the net and decipher its contents. "A sniffer can read every keystroke sent out from your machine, including passwords"

CHOOSING GOOD PASSWORDS – WHAT NOT TO DO

- What NOT to use: words, proper nouns, or foreign words, avoid words with a number tacked on at the end. No personal information (names, pets, addresses, phone numbers, etc)
- A strong, effective password requires a necessary degree of complexity. Three factors can help users to develop this complexity: length, width & depth.
    - Length: It is generally recommended that passwords be between six and nine characters. Longer passwords are harder to crack. Simply put, longer is better.
    - Width: Width is a way of describing the different types of characters that are used. (uppercase, lowercase, numbers, special characters, etc)
    - Depth: Depth refers to choosing a password with a challenging meaning – something not easily guessable.

CHOOSING GOOD PASSWORDS – WHAT TO DO:

- Stop thinking in terms of pass*words* and start thinking in terms of *phrases*. "A good password is easy to remember, but hard to guess." (Armstrong) The purpose of a mnemonic phrase is to allow the creation of a complex password that will not need to be

written down. What may be most effective is for users to choose a phrase that is has personal meaning (for easy recollection), to take the initials of each of the words in that phrase, and to convert some of those letters into other characters (substituting the number '3' for the letter 'e' is a common example).

- Example: the phrase "A good password is easy to remember" can translate to: Agp1e2r
- Example: "Our family loves to go to Hawaii" can translate to: ofL2g2h, or 0Fltg2H

– Avoid using the same password on multiple accounts. Doing this creates a single point of failure, which means that if an intruder gains access to one account, he or she will have access to all of the user's accounts.

– Users should never disclose their passwords to anybody unless they know them to be authorized (i.e., systems administrators). Even then, passwords should only be disclosed in person (not over the phone or by e-mail) to a known, trusted source.

– If possible, do not write your passwords down.

- In order to ensure their ongoing effectiveness, passwords should be changed on a regular basis. How often one should change passwords really depends on the account. Online financial accounts should be changed every month or two. Corporate network passwords should be changed every 3-4 months.

Some Interesting Reading:

- How To Create The Perfect Password
  https://www.theguardian.com/money/2016/may/21/how-create-perfect-password-hackers-online-accounts-safe
- The Simplest Security: A Guide To Better Password Practices
  http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices
- The Secret Life of Passwords
  http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html?_r=0
- Password Protection: How to Create Strong Passwords
  http://www.pcmag.com/article2/0,2817,2368484,00.asp
- What is YOUR Password? Jimmy Kimmel
  https://www.youtube.com/watch?v=opRMrEfAIiI
- SplashData - Worst Passwords of 2015
  https://www.teamsid.com/worst-passwords-2015/