Security: Your Password, Your Money, Your Friends– Safety (4.26.15)

From: Your writer is a veteran of information technology and information security. Some years back we ran nightly password cracking sessions. Many passwords are (and were, then) very weak and easy to guess (or crack) in minutes or less. Easy (bad) passwords contained words, names, phones, licenses and dates.

For you: Today an army of bad guys are trying to guess your password. If the same password is used two or more places, bank, investment, social sight, one cracking success can injure you two or more places. That can cost you money, your credit, even a place on your friends' "Blocked Sender Lists", or, worse, a bad guys list.

What: We have all had mail from John or Jane who lost their money, passport or plane ticket in London, Rio or wherever. That is only one of a myriad of scams sent from the accounts of friends with bad (lost) passwords. If you are lucky you only aggravated your friends, gave up their email address and at worst need to get a new email account name, perhaps with another email provider, **AND, CREATE A STRONG PASSWORD**, which you change every 60 to 120 days.

Passwords: If you haven't seen and read the PASSWORD SERMON, here it is:
- Eight character passwords are risky, **10 to 14 character passwords** are much better.
- **Use no: names, dates, words in ANY language, repeating letters or numbers.**
- You might create your own ACRONYMS (mixed with numbers and punctuation).
- Use at least **2 of A-Z, 2 of a-z, 2 of 0-9, 2 of Special Characters !@#$%&_-;:+**.
- **Mix** numbers, punctuation, upper and lower case characters.
- **Change passwords** on 60 to 120 day cycle.
- **Do not share** or write down your password where it can be found,
- **Do use** a secure password keeper.
- **DON'T click** on links, anything you don't know what it is or who it is from.
- **USE DIFFERENT Passwords:** If you have many passwords, don't use the same password two places, ONE LOST IS MANY LOST.

Web Browsing: Many browsers let you reveal headers, origin information and even source showing you phony links. (show headers, show source). Bad links look good until you see their source (numbers, wrong country, unknown sender).

Keeping and generating passwords: Smart phones, tablets, PDAs Windows, MAC and Linux computers allow you to use inexpensive password keepers. These do not store your password cache on the web for others to crack. I use *SplashID*[1]. There are others. PC World[2] magazine likes Agile Web Solutions' *1Password*, *Clipperz*, *LastPass* and *RoboForm* from Siber Systems Inc. [They] tested each on four different platforms: a MacBook Pro running OS X 10.5.8, laptops running Windows 7 and XP, and an iPad. [They] also tested browser add-ons for Internet Explorer, Firefox and Chrome.

1 Runs on most platforms http://www.splashdata.com/**splashid**/

2 (http://www.pcworld.com/article/208113/Best_Password_Managers_Top_4_Reviewed.html)