

Your Password, Your Friends, Your Money – Safety (2.13)

From whom: Your writer is a veteran of information technology and information security. Some years back we ran nightly password cracking sessions. A large percentage of passwords are (and were, then) very weak and easy to guess (or crack) in minutes or less. They 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 Lists", or, worse.

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 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 90 to 120 days.

Passwords: I don't know if you have seen and read the PASSWORD SERMON, or not, but, here it is:

- Eight character passwords are okay, **10 to 14 character passwords** are much better.
- Use **no words in any language**.
- 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 90 to 120 day cycle.
- **Do not share** or write your password where it can be found.
- **DON'T click** on anything you don't know what it is or who it is from.

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).

All different passwords: If you have many passwords, don't use the same password two places.

Keeping and generating passwords: Most smart phones, PDAs and 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. There are others. PC World (http://www.pcworld.com/article/208113/Best_Password_Managers_Top_4_Reviewed.html) 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.