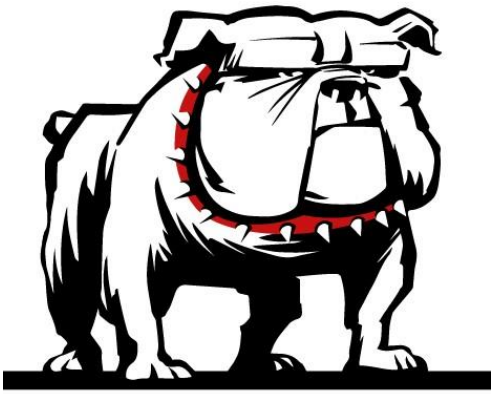

Passwords – the Watchdog of your Systems

Having good, strong passwords is the first line of defense for your systems and data. Multiple and complex passwords on your applications is like having a watchdog or security system on your home. Criminals are less likely to pursue targets with robust forms of security. A home with a barking dog or posted home security sign, is a less likely mark for a thief, just like a desktop that makes use of robust passwords on applications and data becomes an unappealing target for a hacker.

But what exactly constitutes a hardy password that hackers will avoid? To answer this, we must first understand the motivation and tools of a hacker. Make no mistake, a cybercriminal's sole intent is to steal from you. They gather as much information about you as possible and then either sell it or use it to gain monetarily at your expense.

Cyber criminals use many tools to achieve their goals including:

- smart tables of words/phrases that try to guess your password
- phishing emails with fake login pages that skims your password
- social engineering tactics like calling an office posing as an IT security tech asking for the network access password
- malware like a keylogger, or screen scraper, which records everything you type or takes screenshots during a login process

A common but false notion is that you are not a target because you don't have much to take. For a hacker, it is more about the volume rather than the value of the victim. For example, a bike thief will go down a line of chained bikes with bolt cutters and take every bike he can, regardless of the value of the bike. He doesn't have time to assess the worth of the bikes, he is just going to steal the ones with the locks that can be compromised. Those who invested in strong locks will be spared.

How can we discourage a hacker? Invest in strong locks – passwords! After wasting time on too many failed attempts trying to crack a password, a hacker will move on. Here are some tips for strong passwords:

- Utilize multifactor authentication whenever available. Many applications or sites that require a login will offer this additional level of security. There are also products like DUO that will help secure your remote access.
- Change your passwords often and do not use the same password on every application. Long complex "passphrases" are recommended and tend to be easier for users to remember.
- Don't save your passwords in a file that is not secure. Many people create a word, excel or text file and name it something like mypasswords.doc. A file like this can be immediately detected by a hacker.

For more information, call Right Click Solutions.

Right Click Solutions LLC
small business computer consulting

27 Radio Circle Drive, Suite 104 Mount Kisco, NY 10549 (914)242-3212 www.RCSLLC.net