Making Secure Easy-to-Remember Passwords

Philip Braunstein

December 14, 2015

Abstract

We like to imagine that computer security is usually compromised by genius hackers exploiting inscrutable vulnerabilities. Often however, a bad guy breaks into a computer because the password to that computer is written on a note next to the computer. Shoring up technical security is a worthy cause, but this effort is rendered irrelevant unless we minimize the impact of social engineering resulting in password leaks. People avoid changing their passwords, leave them written in plain text in a document on their computer or even on a sticky note on their computer for one reason only: secure passwords are hard to remember. Most passwords considered secure are strings of random characters that are nearly impossible to remember. Three password-making strategies are evaluated in this report: random strings of characters, numbers, and symbols; abbreviations of phrases mixed with meaningful numbers; and an adjective-noun-verb-adjective-noun string modeled after xkcd 936. Passwords are evaluated on ease of memorization, cryptographic strength against a password cracker, and bits of entropy