**The Fulcrum Group, Inc.**
**(817) 337-0300**

# Password Tips & Tools

## 8 Sm@rt Th1n9s Ab0ut Pas$w*Rds

This White Paper is brought to you by your friends at

The Fulcrum Group, Inc.

THE FULCRUM GROUP
*One Technology Solution: Yours*

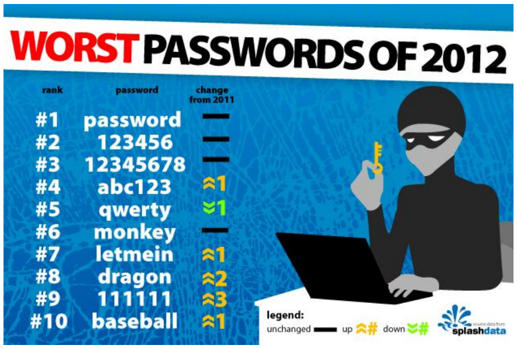
# Password Tips & Tools

## 8 Sm@rt Th1n9s Ab0ut Pas$w*Rds

### *Oh no, you didn't…*

**1.** Here are some interesting facts gleaned from a recent study.

- 4.7% of users have the password *password*; 8.5% have the passwords *password* or *123456*;
- 9.8% have the passwords *password*, *123456* or *12345678*;
- 14% have a password from the top 10 passwords.
- 40% have a password from the top 100 passwords.
- 79% have a password from the top 500 passwords.
- 91% have a password from the top 1000 passwords.



WORST PASSWORDS OF 2012

| rank | password | change from 2011 |
|---|---|---|
| #1 | password | — |
| #2 | 123456 | — |
| #3 | 12345678 | — |
| #4 | abc123 | ↑1 |
| #5 | qwerty | ↓1 |
| #6 | monkey | — |
| #7 | letmein | ↑1 |
| #8 | dragon | ↑2 |
| #9 | 111111 | ↑3 |
| #10 | baseball | ↑1 |

legend:
unchanged — up ↑# down ↓#

source data from splashdata

http://xato.net/passwords/more-top-worst-passwords/

### Length+Variety+Randomness+Uniqueness=Password Success

**2.** Security experts generally agree that a strong password must have four components: length (longer = stronger), a variety of character types and cases, randomness, and uniqueness. "Every password you use can be thought of as a needle hiding in a haystack," says data security expert Steve Gibson. "After all searches of common passwords and dictionaries have failed, an attacker must resort to a 'brute force' search— ultimately trying every possible combination of letters, numbers and then symbols until the combination you chose is discovered."

### *The Facts*

**3.** According to research from Microsoft, the average computer user has 6.5 passwords, each of which is shared across 3.9 different sites. Each user has about 25 accounts that require passwords, and types an average of eight passwords per day.

### *Longer Passwords Double the Effort Required to Crack Codes.*

**4.** The average password requires about 240 attempts to exhaust all possibilities during a hacker's brute force attack. However, a hacker using a brute force attack will typically have to try half the possible passwords before finding the correct one (password-detection programs can run several billion password guesses per second.) Adding just a single character to a password doubles the number of guesses required, which is why longer passwords are far more secure. In short, *the longer the password, the better for you*.

THE FULCRUM GROUP
*One Technology Solution: Yours*

### *You Can Be Discriminating With Your 'Best' Passwords.*

**5.** You don't need a strong password for every site. Just for the important ones. Slate.com tech writer Farhad Manjoo says four or five passwords will suffice, as long as your strong and unique ones are used for the important accounts. "It's perfectly OK to repeat passwords on sites that don't need to be kept very secure," says Manjoo. *But never reuse your business network, email, or online bank account passwords. Those should always be unique*.

### *DtwRnMA? (Does The World Really Need More Acronyms?) – YES!*

**6.** Manjoo has a helpful shortcut for creating passwords that are both strong and easy to remember.

"Start with an original but memorable phrase …
and turn [it] into an acronym. Be sure to use some numbers and symbols and capital letters, too.

I like to eat bagels at the airport becomes Ilteb@ta, and My first Cadillac was a real lemon so I bought a Toyota is M1stCwarlsIbaT."

### *Be Familiar With Phishing*

***7.*** Phishing is the act of attempting to acquire information such as usernames, passwords and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. And remember, your bank will NEVER ask for personal information like your password, account number, or social security number via email. As always, be fiercely protective of your personal information electronically (and otherwise). The APWG's website has continuously updated information on the latest in phishing scams and cybercrime. Visit here for current tips to avoid phishing:
http://apwg.org/resources/overview/avoid-phishing-scams

### *Use Intruder Lockout if necessary.*

**8.** Owners of web-based services and apps have access to additional tools to ensure the security of user data. A simple and effective solution to help prevent brute-force attacks is to have an automated intruder lockout system in place so that when the wrong password is entered multiple times in a row, the account will be locked.

## Contact the Fulcrum Group today at 817.337.0300 for more information and to ensure your organization is adhering to security best practices.

THE FULCRUM GROUP
*One Technology Solution: Yours*