In A Nutshell…

Strong Passwords

Why do I need a strong password?

We live in a time where almost everything can be done online. Most of us have at least one online account and many of us have more. These accounts usually require a password to access the information. Passwords provide the first line of defense against unauthorized access to your accounts, computer, or other password-protected information. The stronger your password is, the more difficult it is to figure out.

Hacking a password

In 2011, Businessweek posted an article titled, "The Problem with Passwords", which provided information about the most commonly used passwords and the estimated time it would take a hacker's computer to randomly guess your password based on its strength.

☑ Users who choose a common word or simple key combination for a password: 50%

☑ Time it takes a hacker's computer to randomly guess your password:

Password Length	If all lowercase letters used	If uppercase letters were also used	If numbers and symbols were also used
6 characters	10 minutes	10 hours	18 days
7 characters	4 hours	23 days	4 years
8 characters	4 days	3 years	463 years
9 characters	4 months	178 years	44,530 years

**Note: These times reflect only one report based on Businessweek sources. Other articles and data sources have reflected slightly differing times.*

☑ Most-used passwords:

◆123456 ◆ password ◆12345678 ◆qwerty ◆abc123

Mom hacks school's computer system to change kids' grades

A mother, who was employed as a secretary for the Northwestern Lehigh School District (Pennsylvania), logged into the computer system to change the grades of her children. The mother used the district superintendent's sign-on and password to change her children's grades.

Source: usnews.nbcnews.com, 7/19/2012

How do I create a strong password?

Although different business, products, and systems may have specific requirements when creating passwords, the following are best practices when creating passwords:

☑ Make sure your password is at least eight characters in length. Some experts recommend even longer passwords.

☑ Avoid using personal information in your password (name, birthday, account name, etc.).

☑ Make sure your password contains one of each of the following characters:
◆ Uppercase letters ◆Lowercase letters ◆Numbers
◆ Special character or symbols (examples: @ # % ? ! ~ $ + *)

☑ Avoid using dictionary words in any language or words that are easy to guess. The fundamental flaw in passwords is the tendency for most people to select passwords that are easy to remember. In other words, they choose names or words that can be found in dictionaries.

☑ Avoid sequential or repeating characters (examples: 123454678, 88888888, abcdefg).

☑ Avoid recycling or reusing passwords.

☑ Create a passphrase instead of a password. A passphrase is similar to a password but is usually longer. Passphrases are usually a string of words/texts or a sentence.

Where can I get more information?

U.S. Computer Emergency Readiness Team (US-CERT), Department of Homeland Security	
Security Tip (ST04-002): Choosing and Protecting Passwords	http://www.us-cert.gov/ncas/tips/ST04-002
“Password Security, Protection, and Management”	http://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf
Weak Passwords/Hacking Passwords	
Time Magazine *“These Are the 25 Worst Passwords of 2012”* This article lists the 25 worst passwords of 2012. Are you using one of them?	http://techland.time.com/2012/10/25/these-are-the-25-worst-passwords-of-2012/
Lifehacker.com *“What Professional Password Guessers Look for in Your Password”* This brief article explains how professional password guessers hack passwords.	http://lifehacker.com/5800346/what-professional-password-guessers-look-for-in-your-password
“How I’d Hack Your Weak Passwords” This article provides more details as to how one internet expert would go about hacking weak passwords.	http://lifehacker.com/5505400/how-id-hack-your-weak-passwords
Strong Password Tips	
Thegeekstuff.com *“The Ultimate Guide for Creating Strong Passwords”* This article contains tips and guidelines on how to create strong passwords and for avoiding weak passwords.	http://www.thegeekstuff.com/2008/06/the-ultimate-guide-for-creating-strong-passwords/
Microsoft Information, from Microsoft, for creating strong passwords	http://www.microsoft.com/security/online-privacy/passwords-create.aspx

Hawaii State Department of Education ◆ Data Governance Office
P.O. Box 2360 ◆ Honolulu, HI 96804
P: 808.218.6791 ◆ F: 808.440.2859
E: DGO@notes.k12.hi.us

Data Governance Office Websites
Public content
http://www.hawaiipublicschools.org/VisionForSuccess/SchoolDataAndReports/HawaiiDataSources/Pages/Data-Governance.aspx

Employee-related content
https://intranet.hawaiipublicschools.org/offices/dgo

Updated: 3/3/2014