HEADSTRONG PASSWORD GUIDANCE

Center for Technology Innovation
Texas Hospital Association

We all know the importance of using passwords to protect against unauthorized access to personal information. Passwords should be secret, sufficiently complex and not written down. But with a growing number of applications and systems protected by passwords, particularly in health care, it can be challenging to meet this standard.

Faced with corporate password rules, compliance requirements and the need to remember multiple passwords, individuals have resorted to any number of creative ways to manage. Password managers and similar software solutions are popular but inherently risky because they share a common weakness with the use of the same password across multiple systems. If a bad actor figures out the one password, he or she has access to all of your systems.

The Texas Hospital Association's Center for Technology Innovation developed a better solution. We created an approach called "Headstrong Passwords." Built on the premise of a "pass phrase," rather than a password, this method: 1) delivers strong passwords that are easy to remember and 2) ensures that each system used has a unique password.

Here's how it works:

Step 1 – Forget about pass "words" and come up with a pass "phrase." This should be a phrase with six to eight words that you will never forget. This can be a personal mission or philosophical statement, a line from a movie, famous quote, etc. Longer phrases are better. Derive your base "password" by selecting the first letter of each word in the phrase. For example: "Land of the free, home of the brave" becomes the base password "Lotfhotb."

Step 2 – Build a personal substitution cypher.

Example:

Character	**Substitution**
Letter "o"	@
Letter "t"	!
Letter "b"	6

*IMPORTANT: CREATE YOUR OWN SUBSTITUTION CYPHER. Very important that you memorize the substitution cypher. You will use it for life.

Step 3 – Apply your substitution cypher to your password. "Lotfhotb" becomes "L@!fh@!6".

ABR

Step 4 – Build a personal abbreviation system.
For each system you have an account, create an abbreviation that follows a specific rule. For example: Use the first three letters of the name of the system, all caps.

System	Abbreviation
Austin Power	AUS
Bank of America	BAN
Gmail	GMA

Step 5 – Identify a logical break in the password to insert the system abbreviation.
In the phrase “Land of the free, home of the brave” there is a natural break after the first four words, which is a good place to insert the abbreviation. Accordingly, “L@!fh@!6” becomes the following passwords for the three systems above:

System	Abbreviation	Password
Austin Power	AUS	L@!fAUSh@!6
Bank of America	BAN	L@!fBANh@!6
Gmail	GMA	L@!fGMAh@!6

Step 6 – Additional Concepts:

- *Some passwords that have to be reset at intervals:*
  For systems that require passwords be reset on a scheduled interval, you must develop an additional method to vary your password. Suggestion: Append or insert in the password two to three characters that add variability. For example, add two to three digits for the month you reset the password (e.g. “10” or Oct) as a prefix, suffix or inserted in-line.

System	Password
Austin Power	L@!fAUS10h@!6
Bank of America	L@!fBAN10h@!6
Gmail	L@!fGMA10h@!6

- *Passwords for low-security systems:*
  Low security systems, such as newspaper or magazine web sites, or any other systems where you do not store PHI or PII, do not require “Headstrong Passwords.[1]” Instead, choose a password that is easy to remember.
  IMPORTANT: This password should be different and unrelated to your headstrong password.
  Suggestion: name of your favorite football team, car, vacation spot, etc. Avoid using personal information such as the name of your children, parents, date-of-birth, and pet names as these are frequently security question items.

- *Systems that have password rules which limit the use of special characters or impose other password rules which conflict with your “password”:*
  If this is a rare occurrence, alter your substitution cypher and SAVE this password. Do not write down the password but rather write down the variability you need to remember. For example, if the system in question does not allow the use of the “@” symbol (or special characters) in a password, then substitute the special character with some other acceptable character, such as the number “6”. If you have multiple exceptions, make multiple substitutions. If this is happening too frequently, consider re-setting your passphrase.
  Suggestion: The logon for widget.com is headstrong @=6. In this manner you’re writing down the key to that password without revealing your password.

[1] Headstrong Passwords is trademark pending from Texas Hospital Association. All rights reserved.