

dos and don'ts of password creation

Hackarazzi Hit Home! Why Celebrity Password Hacking Matters to You ... and How to Protect Yourself and Your Accounts

Not long ago, the media was buzzing with news of a 35-year-old Florida man who managed to hack into the email accounts of as many as 50 celebrities, stealing their passwords and breaking into their address books and financial accounts, among other things. He was able to guess their passwords by mining social networking sites, magazine articles and more to glean personal information about them, (which they had used to create passwords) and by using sophisticated "brute force" hacking software.

This story hit the news with such force because of the high-profile names of the victims, who included Scarlett Johansson and Kim Kardashian. But it is far from an isolated case. The FBI has been dealing with several similar cases in recent months, not necessarily involving such prominent victims.

With more and more people participating in social media, we have all become increasingly vulnerable to this type of destructive hacking. Once someone discovers your email password and/or figures out the answers to your challenge questions (Who was your first pet? Where did you go to high school? What is your father's middle name?), it is relatively easy to capture everything you do via email, and even follow you as you change passwords.

For this reason, it's critical to choose "strong" passwords that are hard to guess. Password strength has been defined as a measure of the effectiveness of a password resisting guessing and brute-force attacks. The longer and more obscure the password, the harder it is to hack. And the more types of characters (including numbers, punctuation, capital and lower case letters, etc.) the better. However, you also need to

For your security, Salisbury Bank's e-Banking service requires your PASSWORD to be between 9 and 25 characters, and must include numbers, letters, and special characters (+ _ % @ ! \$ & * ~ are allowed).

be able to remember your password – and not just one but possibly dozens because it is critical not to use the same password on multiple accounts.

Dos and Don'ts of Password Creation.

Let's just get this over with: the worst password ever is your account number or username. Just don't do it.

Also DON'T:

Use personal information such as your name, birthday, pet's name, school, sister's nickname, or similar information. This stuff is easy to find out via social media or other online sources.

Use anything you can find in a standard dictionary. (Hackers have programs that automatically try dictionary words)

Be clever by spelling your password backward, or using a common misspelling or abbreviation. If you can think of this, so can they.

Use sequences or repeated characters such as 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty). These are not only easy to hack, they're easy for an observer to see as you type them in.

DO:

Make your password as long as possible. Always use at least 6 characters, at least two of which are numeric.

Use as many different characters as possible, including punctuation and, when possible, mixed upper and lower-case letters. (Not all passwords are case-sensitive).

Make sure your password is memorable to YOU.

Microsoft Security has some recommendations for creating long passwords that are easy to remember. They suggest you start with a sentence.

Then:

Remove spaces between the words.

Turn words into shorthand, or deliberately misspell a word.

Add numbers.

As an example, you could start with the sentence "good passwords are easy to remember." Then take out the spaces: "goodpasswordsareeasytoremember." Then shorten some words:

"goodpasswordsrez2remember".

Capitalize some letters.

"goodpasswordsREZ2remember."

Finally, add a memorable number (like the last 4 digits of a childhood phone number):

"goodpasswordsREZ2remember2215."

Taking it a step further, other experts recommend erasing all but the first letter of each word: "gpREZ2r2215." And just to make it even harder for the bad guys, add some punctuation: "gpREZ2r2215!"

Your finished password will even pass muster with the large number of sites that require 6-12 characters and at least one alpha and one numeric.

In conclusion, remember that NO PASSWORD IS UN-CRACKABLE. So use different passwords for different accounts, change your passwords often, and commit them to memory using the methods above. You may not be Leonardo DiCaprio, but your vital information is as tantalizing to others as it is important to you.



www.salisburybank.com banker@salisburybank.com

5 Bissell Street
Post Office Box 1868

Lakeville, Connecticut
06039-1868

t: 860.435.9801
t: 800.222.9801

f: 860.435.0631

This information is provided for informational purposes only and does not constitute legal or other professional advice. We suggest that you consult with a computer expert or technical advisor for guidance with regard to your particular situation. Opinions expressed herein are subject to change without notice. Information has been obtained from sources believed to be reliable, but its accuracy and interpretation are not guaranteed.

© 2011 Salisbury Bank and Trust Company (Form ART-20 December 2011) Member FDIC

Equal Housing Lender