A Simple Guide to Creating and Remembering Hacker-Proof Passwords

Share This Checklist With Your Employees So They Know How To Create Hard-To-Guess

Passwords And Protect Your Organization

By Bob Jenner and Michael Reuben, Ph.D.

A Collaboration of The Network Doctor, Inc. and LA Computer Works.

7 Tips For Creating A Secure Password

You've got one for every site and every application you use--e-mail, online banking, social media sites, and your CRM system, just to name a few. With so many password protected sites to keep track of, the inclination is to always use the same password for every site or to make it so easy you can't possibly forget it (like using Password123). Unfortunately, this compromises all of your data and makes it easy for cyber-attackers to steal sensitive, confidential information.

Studies have shown that password security is still the weakest link in keeping data safe. There are some simple things you can remember when creating a password that can help protect your information.

Use a Password Manager:
One of the best things you can do is to use a password manager. There are many password managers available for you to choose from. Some of the most popular are Roboform, LastPass, Keeper and 1Password. Using a password manager allows you to keep all of your passwords securely in one place. With a password manager, all you have to remember is a single "Master password". With this one password, you can access all of your other passwords. Password managers also will automatically fill password protected websites and many applications.

Here are 7 tips to consider if you are creating your own password:

1. Use special characters and numbers, EG: 0-9 and !@#$%^&*
2. Mix up Upper case and lower case letters.
3. Make sure your password is a minimum of 8 to 10 characters.
4. Be sure it's not something that can be guessed easily (zip code, phone number, birthdate, your name, Spouse's name, kid's name, pet's name).
5. Randomly replace letters with numbers, e.g. shake becomes $h@ke.
6. Pick a sentence or phrase, and reduce it to letters of each word only, e.g. "A Golden Key Can Open Any Door Except on Sunday" becomes AGKCOADEO$.
7. You can also use disconnected words as your passphrase. Horse!Chance.Dont,backwords-run!!!!

Make It Poetic

Everybody has a favorite poem or song that they'll never forget. It might be from Shakespeare, Hemmingway, the Beatles or the Rolling Stones. Whatever the stanza or verse, you can turn it into a password. Here's how.

Start by writing down the first letter of each syllable, using capital letters for stressed syllables and keeping any punctuation. Let's try this line from Romeo and Juliet: "But soft, what light through yonder window breaks?" From that, you'd get *bS,wLtYdWdB*? You could add *A2S2* for Act 2, Scene 2, if that's something you'll never forget. Or *1597* for the year of publication.

If the passage doesn't have a strong meter, you can just take the first letter of each word, using the existing punctuation and capitalization. Starting with the quote "Be yourself; everyone else is already taken. - Oscar Wilde", you could come up with *By;eeiat.-OW*. Adding a memorable number rounds out the password, perhaps *1854* (his birthdate) or *1900* (his death).

Your poetic password will be completely different from these examples, of course. You'll start with your own meaningful song or quotation and convert it to a unique password that nobody else could guess.

When you make long and complex passwords that are not easy for a hacker to guess, you make it much harder for a hacker to guess. When you add extra random characters that are not in a word like vxrvffc, hackers can’t be successful using dictionary words. A process called a “Brute Force” attack.

Not all cyber-attacks can be avoided, but don’t make it too easy for them. Be proactive and update all of your passwords so they meet this kind of criteria. Also remember, don’t use the same password on multiple sites! If you do, and one get’s compromised, they are all compromised!.