Passwords

Professor Don Colton

Brigham Young University Hawaii

Cracked: 11151982, 4glory, ALOHA, carlos, cheerio, daniel8, is351, marathon, monster, surfer, tevita

How do you pick a good password? And who cares?

There are many sources of password advice. This is a short summary that should help you pick a good password.

Hackers are constantly attacking web servers and other network resources in the attempt to "own" them so they can be used for sending spam, carrying out distributed denial of service attacks, or doing other bad things. Most days we are probed hundreds of times by hackers looking to break in. We do not want to become a victim.

To stay one step ahead of the hackers, on the IS2 machine we run our own password hacking program to test all passwords for ease of break-in. If we break your password, we assume a hacker could too. So we warn you to secure your account better, and if you don't fix it we suspend your account to protect ourselves.

The cracked list above a partial list of actual student-chosen passwords that were cracked by our password hacking program. Those would be examples of bad passwords.

Here are some rules for picking a good password:

* The key thing is that your password should be (a) easy for YOU to remember, (b) hard for someone who sees it to remember, and (c) hard for anyone to guess.

* Especially avoid dictionary words. These are the first things that hackers try. Dictionary is not limited to English.

* I recommend that you use the initial lettes of a phrase you can remember. For example, "I Nephi, having been born of goodly parents" might become "INhbbogp".

* Modify your password by replacing some letters with digits or other special characters. For example, "INhbbogp" might become "1Nhb20gp" where we replace the "I" with a digit "1", the two "b"s with a "b2", and the letter "o" with a digit "0".

* Here are some popular character swaps to get you thinking: A=4=@ B=%=8=6 E=3 G=6 I=1(one)=l(el)=! K=1¡=x O(oh)=0(zero) q=9 er=0r S=$=5 T=7=+. Anything that looks graphically similar would work.

* Change your password if you think it has been discovered. Some places require passwords to be changed every six weeks or at some other set interval. There is little or no evidence that this improves security. Many users simply alternate between two passwords, as in Aloha1 and Aloha2. Others append the date to their password, as in AlohaJan, AlohaFeb, AlohaMar, etc. Is that really any more secure? Well, maybe a little. But password cracking programs will probably not be fooled.

1 Authentication

Computers facilitate access to resources. Before computers we dealt with humans, typically on a familiar basis. They knew us. We did not have to prove who we were when carrying out business. When you borrow $5 from your friend, he probably does not ask to see your ID.

But when you ask for $20 from the cash machine, it wants your ID card and your PIN number. Why is that? Because the computer does not know who you are.

Is it possible for you to give someone your bank card and have them get the $20 from the cash machine? Sure, if you trust them. Give them your card. Tell them your PIN. Let them handle the transaction.

The purpose of the bank card and the PIN number is authentication. Anyone who has both those items will be presumed to have the right to use them.

The key to a door is typically a single token of authority.

The bank card and pin are two tokens that must be used together.

In general, a token is something you are, something you have, or something you know.

Things you are would include finger prints and retina scans. It could include the length and shape of your fingers and toes. It could include the way you walk or the shape of your body. It could include your voice print. Sometimes these are called biometrics.

Things you have would include keys, driver's licenses, and temple recommends.

Things you know would also be called "shared secrets." When I am trying to prove to you that I am me, I could tell you something that only you and I know. That would be evidence of my identity. The combination of a lock is a shared secret. The PIN number with your bank card is a shared secret.