

Why We Need a Stronger Password

The standard line that people use to justify not having a proper password policy is:

"I don't have valuable data that people would want to take".

We have all been there, we use a simple word, or the dog's name or a favorite team as a password because we don't think it matters, we think that nobody is going to want to crack into this account; and even if they did, what would it get them?

Even if you do not have lots of bank transactions stored on our network that doesn't mean that there isn't valuable data stored there. A quick list of the possibilities might include client credit card data or employee social security numbers or other confidential information. Would you really want everything on our network to be available to a thief? The answer is most likely no.

It may not even be a physical person who is trying to crack the passwords; it might just be a piece of software that scans for passwords and users name combinations that work. Your network may not seem interesting to you, but to a software program, you are just another number in the crowd, a number to be scanned and tested and cataloged. Just being on the Internet may be enough reason for a software package to try to crack your defenses.

But what good is a username and password to anyone? Putting aside the confidential data that resides on your network, how would someone take advantage of knowing your username and password?

In the real world, crooks with free access to a physical location can use it to store illicit goods. On the Internet, a valid user name and password is an open door to store illegal software, etc on your network.

One thing that most firms do have that is very valuable is their good name and a public IP address on the internet. SPAM blacklists are lists of Internet addresses that are known for sending SPAM e-mails. A valid user name and password on a network that isn't known for sending spam is as good as gold to the wrong person.

Hackers with no idea who we are still want our server and Internet connection, to use as a platform to attack other networks, spew spam, or store illicit files so they don't get caught with them on their computer.

Suggestion for a standard network password policy:

- Passwords must be changed regularly. Even the best password is no good if someone finds it out. Changing passwords frequently keeps them safe.
- The server will have a history of your recent passwords and won't let you recycle them.
- Passwords will have a minimum number of characters, and not contain your username, first name or last name
- Password complexity filter: Passwords must contain characters from each of the following four groups:
 - (1) Uppercase letters
 - (2) Lowercase letters
 - (3) Numerals
 - (4) Symbols (characters that are not defined as letters or numerals, such as !, @, #, and so on)
- Note: this means your password will have to have at least one numeral and one symbol!

The above would be the minimum policy, enforced by the server, but we encourage you to take security seriously and keep your PW hard to crack by following these additional guidelines: No words or names that can be found in a dictionary. Hackers use an automated dictionary attack that can break PWs with common words in seconds. '2lawyers!' would be relatively easy to crack with one of these programs

- No words or names that can be found in a dictionary. Hackers use an automated dictionary attack that can break PWs with common words in seconds. '2lawyers!' would be relatively easy to crack with one of these programs.
- No names or nicknames of your pets or kids - someone who knows you could guess these.
- Don't change your PW by just adding a 1 at the end, then a 2 next time etc. Someone who had your old PW could guess this, making the requirement to change it useless.
- Please don't write your PW on a Post-It and stick it to the bottom of your keyboard or in your desk drawer; many networks have been compromised in this way. If you forget your password, a network administrator can reset it for you.

Strategies for creating useful passwords:

So the consensus among security experts is that passwords are one of our greatest weaknesses in the battle against hackers. We want to continually pay attention to our password policies; the problem is that in real life, passwords are a pain. We need some strategies that'll make them easier to live with.

Obviously the main hurdle is to make it both hard to crack and easy for you to remember. A good hacker only needs to crack one password, because he can then install a "sniffer" program that'll capture network traffic, and then run a brute-force hack night and day on a high-speed computer that will eventually crack even the administrator password. So our network is only as strong as our weakest password!

Here are my favorite tricks for this; there are lots of others good ones.

- You can use words and misspell them, using numerals and symbols: Cool dude could become Kew! d00d (nine characters, has exclamation mark, space, and numeral zero) Note, spaces are often OK!
- Take the first letter of each word in a sentence: "I paid five dollars for these shoes!" becomes Ip\$5fts! Make up a sentence about when you moved to Seattle for example, something that naturally has a number in it, and add punctuation.
- A natural sentence, spaces and all, can be good, but I'd like to see at least one word be misspelled so a dictionary hack wouldn't get it. "See sp0t run!" would be good; note the zero instead of o in sp0t.
- When changing a password, you can make a small change; you don't have to start over from scratch. Just try not to make it an obvious change like going from Pa\$\$word1 to Pa\$\$word2.

According to security experts, most password policies are too lax. Spending a little bit of time paying attention the password policies can bring large improvements in your users understanding of network security.

