

## A New Year's Security Resolution My Password is Better than YOur P@\$sword

Some people make resolutions at New Year's time. I resolved to make one next year! Perhaps it is time to resolve to be more secure this year. There are a variety of aspects of computer security that could be addressed, but let's keep it simple for this column and stick to just one resolution — better passwords.

In the past, advice about passwords has often been pedantically correct, yet useless. Let's face it, you are not likely to use a password like "!r4%^s2A", and if you do, you have still failed to create a good one, unless you are on a system with an 8 character limit for the password. The keys to good passwords lie in length (size really matters), and not using a single word in the dictionary, even if it is really long. "Conventional wisdom" dictates passwords that you cannot remember, should not write down, and probably will not use.

Seems like a dilemma. But, good passwords are actually easy. The problem with a password like "!r4%^s2A" is that it is too short. A password like "I really hate passwords" is actually much better. To understand why, let's take a look at how passwords are guessed or "brute force" cracked.

The easiest approach to guessing a password is to find out information about someone and go from there. Spouses name? Pet names, Birthdays? Talk to people and you will find out how truly easy it is to get this information from someone. People who use these passwords are easy pickings. Passwords that are short and pertain to ones personal or even business life are commonly used and easily guessed. Attacks on such passwords are accomplished with simple "social engineering," or with stolen data.

Dictionary attacks try a variety of words found in the dictionary. If you choose the password "January" it will be guessed in a couple of seconds or less by a computer program. You can use real words, but just not one. The art is in combinations, but more on that later.

No matter what you choose for a password it can be cracked eventually with brute force. Brute force simply means trying every possible combination of characters that can be in a password. This is where size really matters. If the password is long enough,



Randy Abrams

a brute force attack will take months or even years.

If you only use lowercase letters and have a 7 letter password there are roughly 8 billion combinations for a brute force cracking program to try. This may sound like a lot, but it can be cracked extremely quickly with a computer. If you use uppercase letters, lower case letters, numbers, punctuation, and special characters, like ¥ or © you are now up to almost 70 trillion combinations. This is still a trivial task for a computer to solve. Now take a look at a password such as "isthisgood". A 10 character password with only lower case letters has about 141 trillion possibilities. So your 10 character lower case password is better than any 7 character password. It is still good to use more than just lower case letters though.

A password such as "8 Resolutions this year!" is 24 characters long, easy to remember, uses 4 different character sets (upper case, lower case, numbers, and punctuation) and is a very hard password to crack with brute force.

One of my favorite techniques uses math equations. Can you remember that  $49+51=100$ ?

This is too short, but what about "Forty9 and 51=One hundred". That's 27 characters! The spaces are legal characters, and if you remember a space at the end you could write the password on a piece of

paper as "Forty9 and 51=One hundred". Note that there was a space at the end of the password that is not seen on the paper reminder. Add 2 to 8 spaces at the end and it is killer.

How about "Was I was born in 1960?" Easy for me to remember (I was), but hard for a computer to crack.

Long passwords mean that it takes a very long time to crack a password, but it can be done. It is important to periodically change your password. Mark Burnett, the author of Perfect Passwords, recommends that once or twice a year businesses and individuals alike have a "password day". Change all of your passwords across your company. If you only change some passwords then an attacker has a lot of time to work on the others. It can only take one known password for a skilled hacker to gain access to the entire network.

Giving credit where it is due, much of this information is from a book by Mark Burnet called "Perfect Passwords", from articles by Jesper Johansson formerly with Microsoft (<http://www.microsoft.com/technet/community/columns/secmgmt/sm1004.msp>), and from numerous discussions with security professionals.

Please do not use any of the examples published as they are now public... and to my boss... sorry about guessing your password! Sigh... There goes my bonus.

If you want to submit questions to "Ask the Expert" please feel free to send them to [askeset@eset.com](mailto:askeset@eset.com).



Randy Abrams is Director of Technical Education for ESET

[AskESET@eset.com](mailto:AskESET@eset.com)

[www.eset.com](http://www.eset.com)

610 West Ash Street, Suite 1900 • San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.