USE PASSPHRASES RATHER THAN PASSWORDS TO GIVE YOU PRIVACY AND SECURITY

Are you currently using weak passwords?

You probably already know not to create passwords using any combination of consecutive numbers or letters such as "12345678", "lmnopqrs", or adjacent letters on your keyboard such as "qwerty." And you've probably heard that using your login name, your spouse's name, or your birthday as your password are also likely breaches of your personal security. In addition, you should never use a word that can be found in any standard dictionary or book of famous quotations, in any language. Crackers use sophisticated tools that can rapidly guess passwords based on words in the dictionary in different languages, even common words spelled backwards.

If you use a common word as your password, you might think you're protected if you replace letters of that word with numbers or symbols that look like the letters such as M1cr0$0ft or P@ssw0rd. Unfortunately, hackers know these tricks too.

Most of Our Passwords are Pushovers!

A survey carried out for the Infosecurity Europe trade show in several years ago found that more than thirty-four per cent of respondents volunteered their password when asked, without even needing to be bribed! The "trick question" that resulted in people revealing their password was, "Does your password have anything to do with a pet or child's name?" Instead of responding with a yes or no, more than a third of the respondents blurted out their password. Very impressive.

Good passwords are absolutely essential for data security. Even the world's strongest encryption (the translation of data into a secret code.) algorithms (a formula or set of steps for solving a particular problem) or logon procedures won't protect you if you use the wrong password.

Even if your passwords once were safe, they may not be today. Passwords that were fine even just a couple years ago may now be vulnerable to attack because of huge advances in hardware and software. Malicious hackers (crackers) now have tools that can make hundreds to thousands of guesses in less than a second. Passwords that might once have taken months or years to crack can now be cracked in hours, minutes, or seconds.

And it takes very little skill to mount a password attack. The simplest form of attack is based on dictionary lists, as noted earlier. The cracking software

simply tries every possible word in a dictionary (including foreign language dictionaries). Any password found in the dictionary will thus soon be discovered. This type of software is extremely simple to create because no deep analysis or cryptographic skill is needed to defeat many passwords!

Similarly, passwords based on common phrases are very weak. A cracker can use a dictionary of famous quotations in much the same way as using a dictionary of individual words. Thus, any password based on familiar quotes is likewise easily discovered.

It's only just a little more complicated for a malicious hacker to cover the most common permutations and variants of words and phrases. For example, some people choose a password or phrase, and then touch-type that word or phrase, but shift their hands one character to the right, left, up, or down from the normal typing position. The resulting output looks like gibberish, but really isn't. It retains a regular pattern that a computer easily can sniff out.

At a quick glance, “-wee305r" looks like a pretty good password, but it's actually not. It's just the word "password" with the keys shifted up one row and to the right as it's typed. A computer can crack that password almost instantly, and yet many people use that simple trick (or others just as easy to defeat) in the false belief that they're safe.

A less obvious word might look harder--- for example, “608fue60j4" is simply the word "touchstone" disguised the same way. But again, a computer will rip through that password in an eye blink.

Similarly, taking a common word or phrase and trying to make it more complex through random capitalization or by appending numbers does little to add real security. For example, in one demonstration, a very slow and antiquated PC running a widely-available cracking tool was able to guess the password "ChEcK12" in only 26 seconds; and today's top-of-the-line PCs could perform the same crack in 1/1000 of a second!

What Makes A Good Password?

So, what makes a good password? There are three major factors: **length**, **complexity**, and **randomness**. We've already touched on **randomness**. A good password will be a truly unique combination of characters, and that means that the password should not appear in any form in any dictionary, book of quotations, and so on. The password also should not be based on simple substitutions or transpositions of common words or phrases: If any underlying pattern remains it becomes easy to crack.

Complexity also is easy to understand. For example, if you limit yourself to the lower-case letters of the English alphabet, each character in your password will have only 26 possible values. Simply allowing uppercase and lowercase letters means that each character in the password can have 52 different values. Add in numbers (0-9) and you have 62 possible values; add the punctuation and symbol characters commonly found on a US-English computer keyboard, and you have a total of about 92 unique (non-repeating) possible values. Clearly, using all the kinds of characters available to you significantly increases the complexity of a password.

Length also is hugely important: A two-character password, where each character could be any of 92 possible values, affords just 8464 (92X92) unique combinations. Three characters allow 778,688 (92X92X92) possibilities; four yields 71,639,296 (92X92X92x92), and so on. So clearly, longer passwords are better because the number of possible character combinations increases exponentially with length.

Online Calculator Will Estimate the "Cracking Time" for Various Passwords

While something like 71,639,296 password possibilities would be daunting in human terms, it's nothing to the brute strength of a PC. An online calculator (located at http://lastbit.com/pswcalc.asp) lets you play with variables to see how long a "brute force" password-cracking program would have to run to defeat passwords of varying lengths and complexities. Note that the "speed -- thousands of passwords per second" figure depends not only on the speed of a given PC, but also on the efficiency of the cracking software, which is a huge variable in itself. But the calculator is seeded with an exceedingly low number, which significantly under-represents the power of today's PC's and software. For a more realistic view of contemporary threat levels, crank up the "speed" variable by several orders of magnitude. (For a hardware-based starting point, you may wish to note that the common Intel P6 is capable of processing hundreds of millions of instructions per second.)

Create strong passwords that you can remember

You could come up with a completely random combination of numbers and symbols for your secure password, but that's not very practical. How would you remember it? Chances are you'd write it down and keep it in the top drawer of your desk and then it's no longer such a great password after all, particularly if it is lost or misplaced.

A strong password is one that is at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess.

Create a strong "passphrase"

The easiest way to create a strong password that you won't have to write down is to come up with a passphrase. A passphrase is a sentence that you can remember, like "Our first home was a small Cap Cod." You can make a pretty strong password by using the first letter of each word of the sentence. For example, ofhwascc. However, you can make this password even stronger by using a combination of upper and lowercase letters, numbers, and special characters that look like letters. For example, using the same memorable sentence and a few tricks, your password is now R1hvv@$((.

If you think that a phrase that you have made up is too hard to remember, you could try a more common phrase, such as "You can't teach an old dog new tricks." If you're using a common phrase make sure to inject at least one number or symbol into the password. Such as "U(+@0dn+".

Other examples of passphrases (passwords)

> 4s@7y@rfbfot(translation: "Four score and 7 years ago our fathers brought forth on this continent."
>
> Anwy((d4yAwy(d4y(…translation: "Ask not what your country can do for you; ask what you can do for your country."