

## RE: Password generators

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-06/0644.html>

---

*From:* Garryck Osborne ([garryck2000@optushome.com.au](mailto:garryck2000@optushome.com.au))

*Date:* 06/28/02

From: "Garryck Osborne" <[garryck2000@optushome.com.au](mailto:garryck2000@optushome.com.au)>

To: <[security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)>

Date: Fri, 28 Jun 2002 14:12:28 +1000

Yep, such passwords are a VERY bad idea... LC4 can ferret these type of substitutions out faster than you can blink (relatively speaking).

May I suggest a different approach to creating a strong password, one that doesn't need to be written down or require a struggle to memorise a string of hieroglyphics.

Take a phrase or sentence of around 10–15 words in length, one that you can easily recall. Here's one lifted at random from an article I was reading: "Of course, not everyone likes to read their email while they're on holiday." Now, take the first letter of each word, (or maybe two from certain words, I'll use two letters and the ' from the word 'they're' in this example) and any punctuation marks can be included as well. Now we have "Oc,nelrtewt'roh." Mangle it a little more by converting some letters to numbers, capitalising certain letters, (I suggest based on emphasis, to make them easier to remember), maybe toss in another symbol or two, whatever you like. In the above example this gives us "0c,nE12rt3wt'Roh." Note that the leading 'O' has changed to numeric zero. This gives us 17 random chars, symbols, numbers, upper and lower case, all the elements of a good, secure password, and will take so long to brute-force that your data will be beyond its use-by date, or you'll have changed passwords long before it can be broken.

After you've done this a couple of times, you'll find that you can create strong passwords on-the-fly, and never need to write them down. They are also MUCH easier to commit to memory.

The following article is well worth a read also. "Choosing Strong Passwords" at <http://online.securityfocus.com/infocus/1319>

One small point from the article; LC (and most other password crackers, so far as I know) is not able to cope with non-printable characters. So, to make a password that cannot even be brute-forced, include at least one non-printing character in your password, as follows:

<quote>

## SecurityFocus BASICS: RE: Password generators

To really increase password strength, use a non-printable ascii character within the first seven characters. ie. within the password 'secret' embed an alt character secret where you hold down the ALT key while pressing the 1,2, and 9 keys on the numeric keypad. NOTE: for laptop users, you'll have to activate numlock and use the j,k,l,u,i,o keys that correspond to the numeric keypad.

</quote>

Garryck

-----Original Message-----

From: [zcat@themall.co.nz](mailto:zcat@themall.co.nz) [mailto:[zcat@themall.co.nz](mailto:zcat@themall.co.nz)]

Sent: Thursday, 27 June 2002 7:41 AM

>

> *Plug in an easily remembered word and it spits out an 1337 version*

> *containing caps, lower-case, numbers, and non-alphanumeric characters.*

NOOOOO!!!!

Surely it's obvious why this would be a BAD password. It's based on a dictionary word, with simple, common letter substitutions. This is the only the next step up (common permutations) from a plain dictionary attack. If you're going to use "h4<Km3" as a password, expect to get hacked.

Don't base your passwords on dictionary words, phonetic misspellings, names, slang, etc. They're all well-known. Use something properly random; I usually do a 'strings -8 /dev/urandom' and then pick something from the first screenful that I think I can memorise. I know people advise never to write down passwords, but I do and keep it down the back of my cellphone for the week or so it takes me to memorise it. IMHO that's still a LOT safer than having an easily-cracked password. But DON'T write it down on a post-it note behind your monitor or under the keyboard!!

- 
- **Previous message:** [Paul Blechschmidt: "RE: NT4 Account keeps getting locked out!"](#)
  - **In reply to:** [zcat@themall.co.nz: "RE: Password generators"](#)
  - **Next in thread:** [Josh Glover: "Re: Password generators"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)