

Q: password generation

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2009-06/msg00296.html>

- *From:* Ralph <grkuntzmd@xxxxxxxxx>
 - *Date:* Wed, 24 Jun 2009 04:49:27 -0700 (PDT)
-

For about 25 years, I have been generating new passwords for my logins by using the following procedure:

- Open an English dictionary to a random page. If the left hand page "tens" digit in the page number is even, use the pattern digit–word–digit–word, else use the pattern word–digit–word–digit
- Open the dictionary to another random page and select the first word (that I recognize :-)) on the left page
- Open the dictionary to another random page and select the first word on the right page
- Open the dictionary to another random page and select the "tens" digit on the left page
- Open the dictionary to another random page and select the "tens" digit on the left page
- Using the pattern selected earlier, form the new password

Recently, I have modified my technique to include "special" characters by using the digits generated to select the character above the appropriate number key on the keyboard (1 = '!', 2 = '@', etc.), choosing whether to use a special character or a number based again on the tens digit of a random page selection.

Is this method "secure"? Are the password reasonable?

I thought of using a similar method to write a generator using a secure random number generator (java.security.SecureRandom or something similar in Python) and a LONG list of English words that I found on the 'net.

Any thoughts?

Are my accounts going to be attacked now that people know how I generated my passwords :-)?

.