

NIH Guidance on Creating a Pass Phrase

In response to increased emphasis on logical access control, some federal agencies have moved away from passwords and switched to “pass phrases” to safeguard their IT systems. It is possible that the Federal government may soon require all agencies to use them.

What’s the difference between a “password” and a “pass phrase”? When you think of a password, people generally think of a word like “Password” or a string of random symbols, such as “R*n]2eB%d” or a combination of the two such as “P@s\$w0rd”. Pass phrases, on the other hand, typically have spaces between words and are longer than the majority of passwords, thus providing extra protection against hackers.

Take a phrase you know and can remember and alter it with character substitutions.

Examples of pass phrases:

- Gr3en EGg\$ @Nd H@mmy!
- My lizard eat\$ 6 crickets daily
- Mix peanuts & oil 2 make peanut butter
- shopping@Macys 4 new furniture
- 2 much talking = big cell phone bill\$

Why is a pass phrase better? From the standpoint of password guessing or cracking, a 5- or 6-word pass phrase is roughly as strong as a completely random 9 character password. However, most people can remember a 6-word pass phrase much easier than a totally random 9-character password. Thus, with more likelihood that it will be remembered and less likelihood that it will be written down, the pass phrase provides better security to protect your computer systems against hackers or automated password cracking programs. Although some older systems might not be able to accommodate a password of phrase length, pass phrases should be used wherever technically feasible.

How can you make a real secure pass phrase? Be creative. Make it personal to you.

- **Use words from a poem, line from a song or a familiar quote with lots of substitutions!** (e.g., Gr3en EGg\$ @Nd H@mmy!)
- Select a phrase that is more than 15 characters and at least 4 words long
- Stay away from common phrases or quotes if not using substitutions.
- Mix short and long words and remember that sentences need not be intelligible
- Character substitutions and/or misspelling strengthen the pass phrase
- Mix languages
- Per the NIH Password Policy, you’ll need to use a combination of at least 3 of the following: upper case, lower case, numbers and symbols. [http://irm.cit.nih.gov/nihsecurity/pwd_policy.doc].
- Exclude some of the spaces between words.

What if I STILL forget my pass phrase? Everyone should be registering at the NIH iForgotMyPassWord website [<http://iForgotMyPW.nih.gov>]. To register, you provide unique answers to five questions. At anytime or any day, *when you’ve forgotten your password/pass phrase*, you can go to that site, answer three of the questions correctly and can then reset your password. If you then need to reset your other, non-active directory, passwords, you can use your NIH Password to log in at Password Reset (<http://silk.nih.gov/passwordset>) where NIH users can reset their Helix, ALW, and Titan passwords. If you need further assistance, contact the NIH Help Desk at 301-496-4357 or helpdesk@nih.gov.