

Password Best Practices

This page is intended to detail some "best practices" to consider when changing your password.

Length

Fairly simply, the longer the better.

Password vs. Passphrase

This is connected with password length, in that the longer the password, the more secure it is. Thus, **b1gb0y97** is no where near as secure as **PresidentN eighborFriend3502**. In addition to being more secure, passphrases have the benefit of being much more memorable than passwords with complexity (e.g. **i** changed to **1** and **o** changed to **0**). Here's a visual explanation as to why:

Complex Password: Tr0ub4dor &3

- UNCOMMON (NON-GIBBERISH) BASE WORD
- ORDER UNKNOWN
- ~28 BITS OF ENTROPY
- $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$
- (PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
- DIFFICULTY TO GUESS: **EASY**
- DIFFICULTY TO REMEMBER: **HARD**

Passphrase: correct horse battery staple

- FOUR RANDOM COMMON WORDS
- ~44 BITS OF ENTROPY
- $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
- DIFFICULTY TO GUESS: **HARD**
- DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

History

- You cannot use the last 10 passwords you've previously used (This is to protect against compromised credentials from continuing to cause problems in the future. It also increases security by forcing work passwords to be different from personal passwords).

Word of Mouth and Pen

- NEVER** tell anyone your password! It is a password for a reason!
- IT technicians should **NEVER** ask for your password. If they do, tell them they cannot have it!
- NEVER** write down your password on a piece of paper, post-it note, or a file on your computer. Anyone with access to your workspace has access to that information, thus it is not secure.

- Utilities exist to manage your multiple passwords in an easy manner. Please contact the [IT helpdesk](#) for more information.

Multi-factor Authentication

In order to reset your password using the Password Reset Portal, you must have a non-MBU email address on file with the University. When you initiate a password reset, an email will be sent to this non-MBU email address with a unique code. That code must be entered to the Password Reset Portal before you can finish your password reset.

For more detailed information about password complexity requirements, click here: [https://technet.microsoft.com/en-us/library/cc786468\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx)

[Password Choice and Security - Additional Resources](#)