Password Best Practices

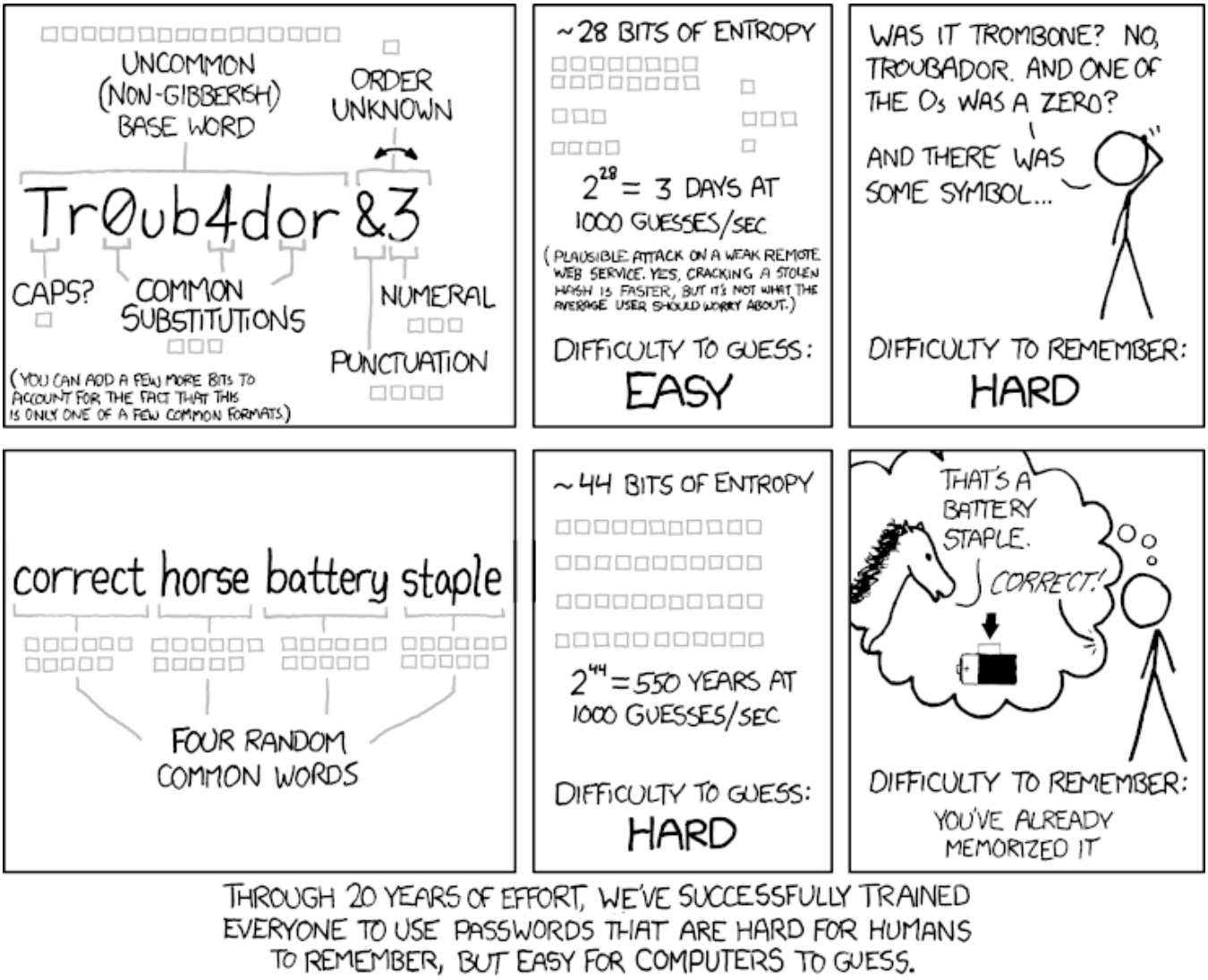
This page is intended to detail some "best practices" to consider when changing your password.

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 **PresidentNeighborFriend3502**. 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:



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

Password Choice and Security - Additional Resources