

# PASSWORD SECURITY

## DIGITAL SECURITY: WHAT YOU NEED TO KNOW

### ELEMENTS OF A STRONG PASSWORD

- Make it **long**: 10 or more characters
- Make it **unpredictable**: consider a phrase combining unexpected words
- Make it **complex**: vary uppercase, lowercase, numbers and symbols
- Make it **unique**: don't use anything you've used before with anything else (e.g. 'My naME is Not MR. MarSter')
- Don't use information others can easily guess about you
- Keep it secret: if you have to share it with someone, switch to a temporary password, share that, then change it back.
- Use symbols, numbers, or multiple languages to make a phrase unique:  
'My naME is Not MR. MarSter'  
'a11 woRk 4nD No p14Y'  
'Let Them Eat 1e gate2L LaunchOcolaT'  
'@ny @ny (are you happy today?)'

### WHY STRONG PASSWORDS MATTER

Sample Password	Time to Decode (Regular Computer)	Time to Decode (Fast Computer)
bananas	Less than 1 day	Less than 1 day
19151466 centuries	19151466 centuries	3990 centuries
We Have No Bananas	19151466 centuries	3990 centuries

*Based on Passfault calculations evaluating password strength*

# PASSWORD MANAGERS

While a little creativity may allow you to remember all of your passwords, the need to change those passwords periodically means that you might quickly run out of creativity.

As an alternative, you can generate random, secure passwords and store them in a portable, encrypted secure password manager.

## HOW THEY WORK

Password manager programs create a private, secure database that stores random, computer-generated passwords for each of your applications and accounts. You can access the passwords manually and copy and paste them to log into an account, or you can install the password manager plug-in on your web browser, which then auto-populates your password when you visit a particular site.

## WHY THEY'RE A GOOD IDEA

Password managers let you:

- Use completely random, computer-generated passwords that are far more complex than regular passwords or passphrases
- Use different passwords for every program and application you access
- In the event of a breach, change *all* your passwords across applications in one central, easy place
- Remember just one single passphrase (to access the password manager) instead of a wide variety of different passwords for different applications.

## ENTERPRISE PASSWORD MANAGERS

[Discussion of enterprise password managers & how they work]

## EXAMPLES

Some password managers vary based on operating system. A good overview and installation instructions are available at [www.securityinabox.org](http://www.securityinabox.org).

- KeePassX
- LastPass
- 1Password

[confirm these/add]

*Adapted from [Security in Box's Password Guide](#) by [Tactical Technology Collective](#) and [Front Line Defenders](#)*