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 ***practical***: make it something you can remember without writing down (unless you use a password manager – see below!)
- Make it ***unique***: use a unique password for each service
- 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.

TIPS TO REMEMBER A STRONG PASSWORD

- Use symbols, numbers, or multiple languages to make a phrase unique:

  'My naME is Not MR. MarSter'

  'a11 w0Rk 4nD N0 p14Y'

  'Let Them Eat 1e gateaU au ch()colaT'
- Use acronyms only you will remember and decode

  '2Bon2B?TitQ' *(To be or not to be? That is the question)*

  'rU:-)2d@y? *(Are you happy today?)*

WHY STRONG PASSWORDS MATTER

Sophisticated computer programs let hackers run through thousands of permutations. A little effort to make a password more complex can go a long way:

Sample Password	*Time to Decode (Regular Computer)*	*Time to Decode (Fast Computer)*
bananas	Less than 1 day	Less than 1 day
bananalemonade	2 days	Less than 1 day
BananaLemonade	3 months, 14 days	Less than 1 day
B4n4n4L3mon4d3	3 centuries, 4 decades	1 month, 26 days
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.

1Password

The best password manager to use is the one that has a user interface which you can understand and which you feel comfortable using. The examples below will use 1Password, but there are various other password managers available today, such as KeePass and LastPass.

1. 1Password can be installed from https://1password.com/downloads/

2. In addition to installing the application on your Windows or Mac computer, we recommend that you install the mobile application to your smartphone as well. You can search in the App store on your phone for “1Password” to find an install the mobile application.
3. 1Password also supports a browser plug in that may help you fill in usernames and passwords on web pages.
4. To learn how to use 1Password, please see https://support.1password.com/explore/get-started/

Adapted from Security in Box’s Password Guide by Tactical Technology Collective and Front Line Defenders