
THINGS YOU SHOULD KNOW ABOUT
PASSWORDS
PASSWORD
Foundation for Media Alternatives
APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

A strong password is your first line of defense for online security.

WHAT ARE THE ELEMENTS OF A STRONG PASSWORD?

1. A password should be difficult for a computer program to guess. ***Make it long and complex.***

2. A password should be difficult for others to figure out. ***Make it practical but do not make it personal. Keep it secret.***

3. A password should be chosen so as to minimize damage if someone does learn it. ***Make it unique and keep it fresh.***

There are a few passwords that you should memorize and that need to be particularly strong. These include:

1. Passwords for your device

2. Passwords for encryption (like full-disk encryption)

3. The master password, or "passphrase," for your password manager

4. Your email password

REMEMBERING SECURE PASSWORDS

It is important to use different types of characters when choosing a password. This can be done in various ways:

1. Varying **capitalisation**, such as: "***iAmYouRmoThEr***"

2. Alternating **numbers and letters**, such as: "***s3cuR1ty***"

3. Incorporating certain **symbols**, such as: "***mYb0dy#MyRuL3s***"

4. Using **multiple languages**, such as: "***M@yTh3Forc3b3W!t#YoU***"

Passwords can also take advantage of more traditional mnemonic devices, such as the **use of acronyms**. This allows long phrases to be turned into **complex, seemingly-random words:**

1. '***To be or not to be***? ***That is the question***' becomes '***2Bon2B?TitQ***'

2. '***We hold these truths to be self-evident: that all men are created equal***' becomes '***WhT2bs-e:taMac=***'

3. '***Are you happy today?***' becomes '***rU:-)2d@y?***'

WHAT IS PASSWORD MANAGER?

It is a tool that can encrypt and store your passwords using a single master password making it practical to use many different passwords on different sites and services without having to memorize them.

HOW DOES IT WORK?

It creates and stores passwords for you, so you can use many different passwords on different sites and services without having to memorize them. It protects all of your passwords with a single master password or passphrase.

CHOOSING A RIGHT TOOL FOR YOU

KEEPASSXC

KeePassXC is an example of a password manager that is open-source and free. You can keep this tool on your desktop or integrate it into your web browser. KeePassXC does not automatically save changes you make when using it, so if it crashes after you've added some passwords, you can lose them forever. You can change this in the settings.

How KeePassXC works? Follow this link: https://ssd.eff.org/en/module/how-use-keepassxc

fma.ph
fma_ph
info@fma.ph
www.fma.ph