Password Manager

Monday, 10 April 2023 20:59

Why using a password manager?

A good password, must be unguessable and long. These 2 features joined to the unwanted repeatability makes this tool very useful. Efficiency and security come together and gives you the ability to store as many different passwords as you want.

Check it out how unsecure are your passwords on the following link

Is secure my password?

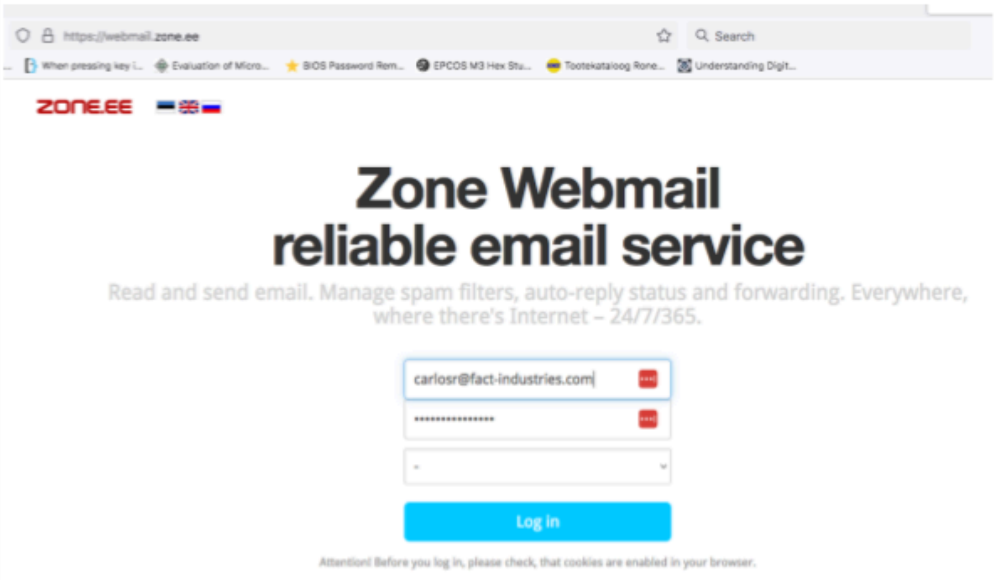
❗	Pay attention to the fact that a long password considered Secure enough like "siemprejuntos", it is contained in many dictionaries, meaning that it is not safe to use.

How convenient is just to know and remember a very strong password that will open the vault of all the others

There are 2 main solutions.

1. Save your passwords locally, which is not that convenient since you only have access to your passwords locally. The common software for this is keePass, which is free and open source. Commonly used in different companies as a password backup.
2. The other one is cloud based. Neither of them are totally free, which makes sense, since they have to maintain an infrastructure to host all users' secrets. You can use LastPass, https://www.lastpass.com/ which offers the option of trying it out in one type of device (desktop devices or mobile phones) for free. To be used in any device is less than 5 € and you can save other important notes.

PM and in particular Last Pass come with browser extensions that automatically render web forms and allow you insert autogenerated passwords that will be saved altogether with the username in your password vault. Browsers' extensions link here.



Zone Webmail
reliable email service

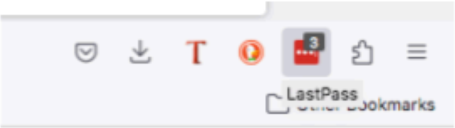
Read and send email. Manage spam filters, auto-reply status and forwarding. Everywhere, where there's Internet – 24/7/365.

carlosr@fact-industries.com

****

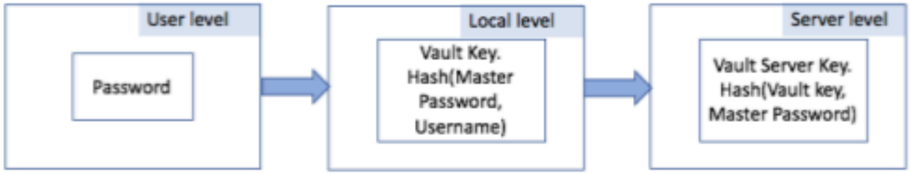
Log in

Attention! Before you log in, please check, that cookies are enabled in your browser.



How cloud based PM encryption-decryption works

Generally speaking, The "key" to enter all the data is encrypted on the client side and then send encrypted to server. This "key" is derived from the "Master Password" to get the "Vault key". **Last pass encryption** is done through 2 steps. First a Vault Key is generated and, it is achieved hashing the username and password (H(username, password)), and iterating them multiple times. Then to authenticate in the server and get our vault, it is used once again, hashed, using your password so, (H(Vault key, password)) and we will call it Vault Server Key. So, with this, is proven that the service provider doesn't possess your master password and eventually, if there is a breach in the server and they can get your data, it is strongly encrypted through hash and iterations, so very difficult to guess.



Security is pretty much depending on your Master Password. You can enhance your MP with a 2 factor authentication login. Last pass offers the use of your fingerprint as a 2nd factor through a mobile app.

Other benefits of using a Password Manager

Other benefits that the passwords managers bring and in particular LastPass is the chance of storing notes, addresses or bank account information. All of them encrypted.