**Passwords, why are they meant to disappear?**

It is safe to assume that nowadays everyone uses Internet and must have come across a login page, in which one has to enter a “password” to access their account. It has become such a mundane step but has any of you wondered if the system has flaws? Can it be improved? And if so, should we be worried?

1. **What is a “password” ?**

In reality, passwords are not something that was coined for our use of the internet, it’s actually much older than that and it can be traced back to the times where we wanted to restrict the access of an area for authorized people only. That meant that someone was standing behind a door and asked the password for anyone who wished to enter.

The system today is roughly the same, with only slight differences, like the ability to have anything as a password, even what appears to look like gibberish, since the verification is made by the service provider through the means of computers.

However even with this little information, we can already point out multiple flaws, and some which are anything but benign. This raises the question: Should we make passwords disappear ?

1. **Why should they disappear ?**

The first issue is that it’s a secret that is shared between at least two entities, if any of them gets compromised the secret is as well, and you shouldn’t be learning anything new when I tell you that the best secret is one that is shared with nobody.

Usually, passwords are passed through a hash function, which is a process that gives a result very easily but makes it very difficult to know what the input was. This mitigates the severity of the issue but it doesn’t fully solve it. Indeed, all it does is make a problem more difficult but far from impossible.

The second issue is that this system relies on your ability to remember the secret. Unless I missed on something, we are all organic living beings with brains, who have the tendency to forget things, amongst those, passwords are forgotten a lot according to a study commissioned by Onepoll on behalf of LastPass, that state that two thirds of participants forget their passwords unless they write it down somewhere, and according to a study from 2019 conducted by Google, 75% of Americans are frustrated by passwords.

If we combine those issues, we can draw a conclusion: Since people tend to forget their password, they avoid making one that is too difficult to remember, and unfortunately a password that is too easy to remember is a password that is too easy to guess. Passwords force us to make a tradeoff between security and convenience. To add insult to injury, we don’t have to remember a password but many, around a hundred. That’s why most use a password linked to a name/date or place, and re-use that same password on every of their accounts, making it very easy to access any of those if you discover what is the password.

So, the question now is, with what can we replace passwords ? We’ll see that there’s plenty of ways of doing it.

1. **How can we replace passwords ?**

If you haven’t figured it out by now, passwords are something that you know. So instead, we should replace them with either something that you have or something that you are. For instance, biometrics are an authentication process that revolve around something that you are. If you have a recent phone model, you may unlock it with your face/eyes or your fingerprints. This is much more secure than a password because the only flaw is if one wants to get into your account, they somehow need to steal your fingers or your eyes… but at that point it’s a separate issue.

To access your accounts online, we refer to that as “Passkeys”, and they can take the form of biometrics but it can also be a physical key, so something that you possess. [Demonstration with GitHub/Microsoft]

1. **Issues ?**

Is it okay to use our body?

Are passwords going to disappear soon?

Is it necessary to go to those lengths?

What if companies refuse to implement this?