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

It is safe to **as**sume that **now**adays **ever**yone uses **In**ternet and must have come **ac**ross a **log**in **pa**ge, in **wh**ich one has to **en**ter a “**pass**word” to get **ac**cess to their **ac**count. It has **be**come such a **mun**dane step but has any of you **won**dered if the **sys**tem has **fla**ws? Can it be **imp**roved? And if so, **sh**ould we be **wo**rried?

1. **What is a “password” ?**

In **re**ality, **pas**swords are not **som**ething that was **coi**ned for our use of the **int**ernet, it’s **act**ually **mu**ch **old**er than that and it can be **tra**ced back to the **ti**mes **wh**ere we **wa**nted to **res**trict the **acc**ess of an **ar**ea for **auth**orized **pe**ople **on**ly. That **me**ant that **som**eone was **sta**nding **beh**ind a **do**or and **ask**ed the **pass**word for **any**one who **wis**hed to **en**ter.

The **sys**tem **tod**ay is **rou**ghly the **sa**me, with only **sli**ght **dif**ferences, **li**ke the **abi**lity to have **any**thing as a **pass**word, **ev**en what **app**ears to **lo**ok like **gib**berish, **sin**ce the **ver**ification is **ma**de by the **ser**vice **pro**vider **thro**ugh the **me**ans of **com**puters.

**Ho**wever **ev**en **wi**th **th**is **lit**tle **info**rmation, we can **alr**eady **po**int out **mul**tiple **fla**ws, and some **whi**ch are **any**thing but **be**nign. This **rai**ses the **que**stion: **Sh**ould we make **pass**words **disa**ppear ?

1. **Why should they disappear ?**

The **fi**rst **iss**ue is that it’s a **sec**ret that is **sha**red **be**tween at **lea**st two **ent**ities, if any of them gets **com**promised the **sec**ret is as well, and you **sho**uldn’t be **lea**rning **any**thing new when I tell you that the best **sec**ret is one that is **sha**red with **no**body.

**Us**ually, **pass**words are **pass**ed **thro**ugh a hash **func**tion, **wh**ich is a **pro**cess that **giv**es a **res**ult very **eas**ily but makes it very **dif**ficult to know what the **inp**ut was. This **miti**gates the **sev**erity of the **iss**ue but it **does**n’t **ful**ly **sol**ve it. **In**deed, all it does is make a **prob**lem more **dif**ficult but far from **imp**ossible.

The **sec**ond **is**sue is that this **sys**tem **rel**ies on **you**r **abi**lity to **rem**ember the **sec**ret. **Unl**ess I **mis**sed on **som**ething, we are all **org**anic **liv**ing **be**ings with **br**ains, who have the **tend**ency to **for**get **thi**ngs, **amo**ngst **tho**se, **pass**words are **for**gotten a lot **ac**cording to a **stu**dy **com**missioned by Onepoll on behalf of LastPass, that **sta**te that two **thi**rds of **par**ticipants **for**get their **pass**words **unl**ess they **wr**ite it down **some**where, and **ac**cording to a **stu**dy from 2019 **con**ducted by Google, 75% of Americans are **fru**strated by **pass**words.

If we **com**bine **tho**se **is**sues, we can **dr**aw a **sim**ple **con**clusion: **Sin**ce **peo**ple **te**nd to **for**get their **pass**word, they **avo**id **mak**ing one that is too **dif**ficult to **rem**ember, and **unf**ortunately a **pass**word that is too easy to **rem**ember is a **pass**word that is too easy to **gu**ess. **Pass**words **for**ce us to **ma**ke a **trad**eoff **be**tween **sec**urity and **con**venience. To add **in**sult to **in**jury, we don’t have to **rem**ember a **pass**word but many, **aro**und a **hun**dred. That’s why most use a **pass**word **link**ed to a **na**me/**da**te or **pla**ce, and re-use that **sam**e **pass**word on **eve**ry of their **ac**counts, **mak**ing it very easy to **ac**cess any of **tho**se if you **dis**cover what is the **pass**word.

So, the **que**stion now is, with what can we **rep**lace **pass**words ? We’ll see that there’s **ple**nty of ways of doing it.

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

If you **hav**en’t **fig**ured it out by now, **pass**words are **som**ething that you **kn**ow. So **in**stead, we **sh**ould **rep**lace them with **ei**ther **som**ething that you have or **som**ething that you are. For **ins**tance, **bio**metrics are an **auth**entication **pro**cess that **rev**olve **ar**ound **som**ething that you are. If you have a **rec**ent phone **mod**el, you may **unl**ock it with your **fa**ce/**ey**es or your **fing**erprints. This is much more **sec**ure than a **pass**word **bec**ause the only flaw is if one wants to get into your **ac**count, they **som**ehow need to **ste**al your fingers or your eyes… but at that point it’s a **sep**arate **is**sue.

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, or put in another way, 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?