Distology.

Why the Future of the Password Is Passwordless

Distology.

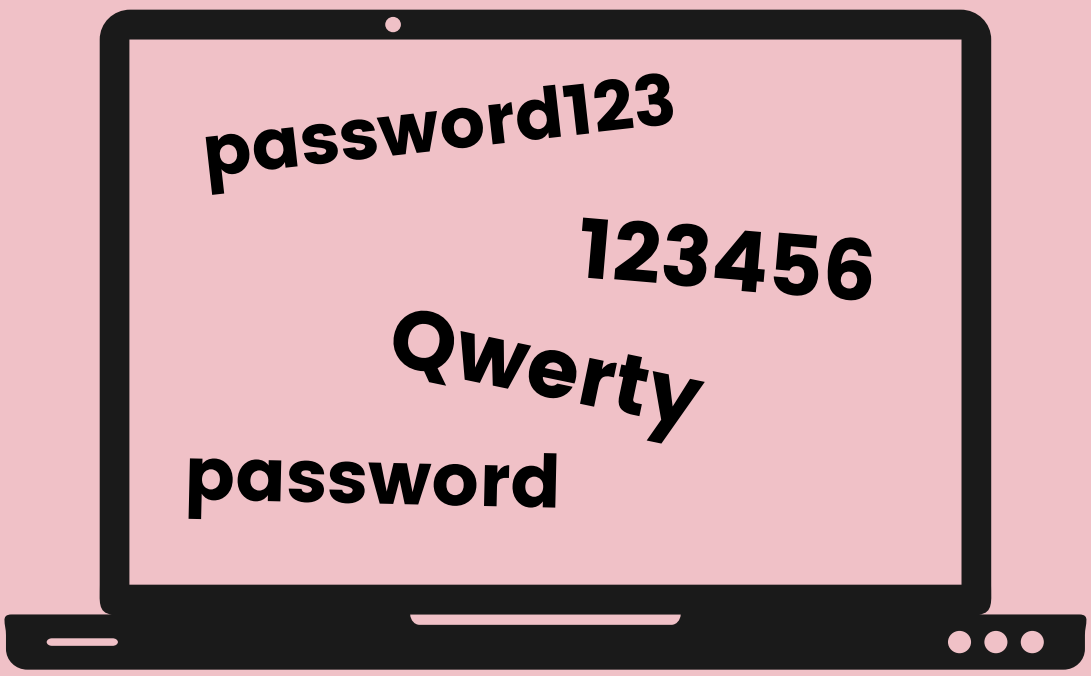
Passwords were first invented as a key to authenticate who you are. However, in the modern world, passwords are now a liability as they are a knowledge-based authenticator, which makes guessing them easy for threat actors.

Distology.

If someone wants to hack your account, it can be as easy as striking up a genuine conversation with you and figuring out what it may be from there - because passwords tend to be something you know as that's easy for you to remember.

Distology.

Another issue with passwords is that we tend to reuse them for our online accounts. Let’s face it, remembering 130 different passwords would be a challenge.



Distology.

But what happens if an online site storing your details gets hacked? Threat actors now have your username and password, which they can now use on other sites.

Passwords alone are a liability.

Distology.

So how do we combat this? We need to add layers of security to our accounts. This is where we introduce MFA (multi-factor authentication).

MFA requires users to prove their identity in more than one way.

Distology.

An example of this is:

- something you know (a pin)
- something you have (your phone)
- something inherent (your biometrics)

Distology.

Think about how much harder it would be for someone to gain access to your account, even if they have your pin, they need to have your phone, and even if someone has your phone, they can't access it without your physical fingerprint. All of this is much safer than a knowledge-based piece of authentication - the password.

Distology.

Going forward, we need to move away from this notion that passwords are the only authenticator. Advancements in technology have allowed us to create new forms of authentication that we couldn’t access when the password was first created.

Distology.

Using a password is like having the key to your home, losing it, and replacing it over and over again.

You will eventually get broken into.