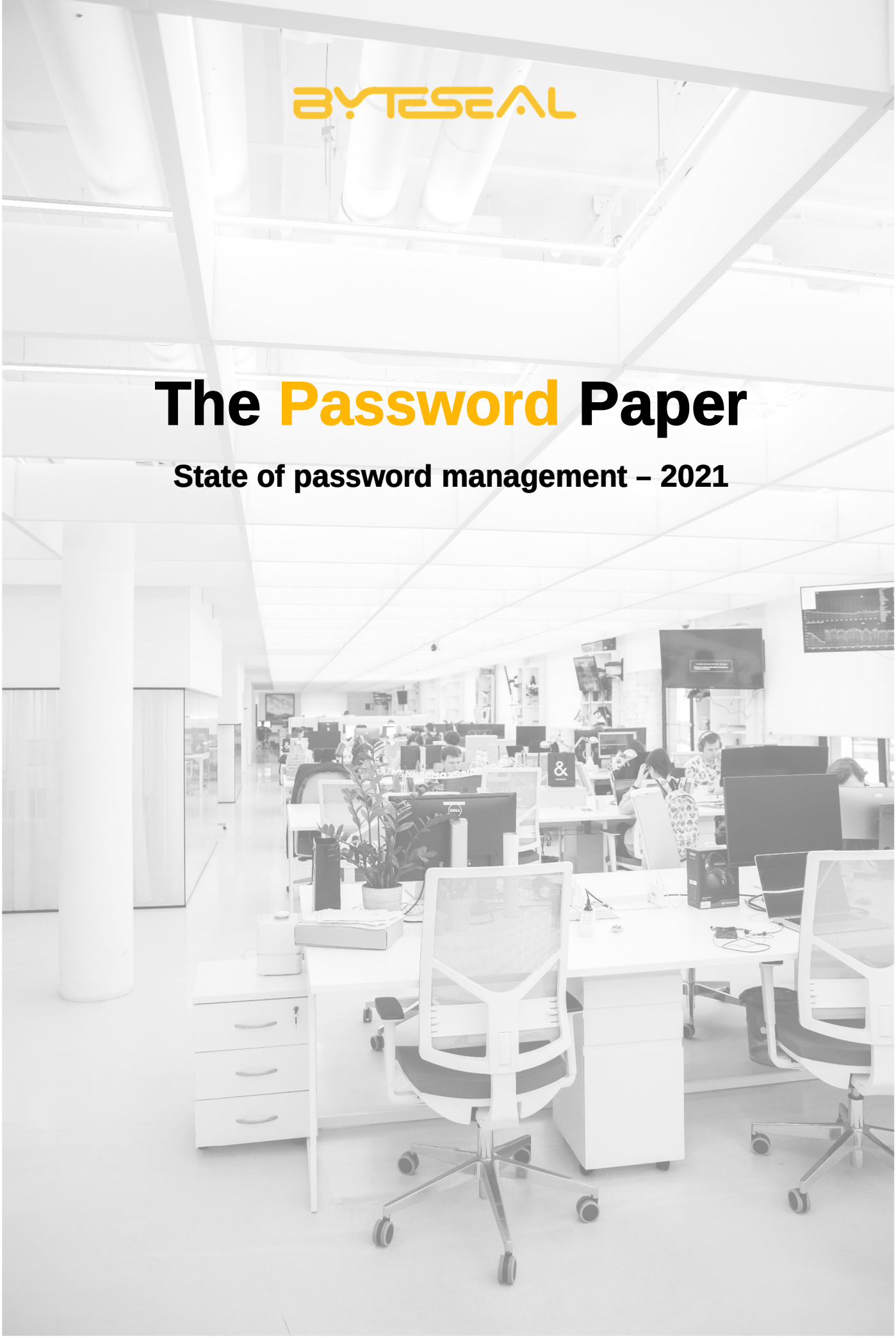
BYTESEAL

# The Password Paper

## State of password management – 2021



# INTRODUCTION

With the rise of SAAS products, the number of login credentials that an organization has to manage is increasing rapidly. At the same time, cybercriminals are coming up with various attack Tactics on a daily basis to steal identities and gain illegitimate access to sensitive information. The easiest way for a cybercriminal to do so is to get access to the users' login credentials. Cyber criminals use various techniques such as phishing, credential stuffing, keylogging, etc. in order to steal the user login credentials. Here are some of the eye-opening statistics regarding credential theft related attacks as shown in Verizon's Data Breach Investigations Report 2021

61% of data breaches involved used stolen passwords and/or weak passwords

85% of the data breaches involved human element

## THE PASSWORD PROBLEM

If we carefully analyze cyber-attacks, we find one thing in common, which is that most attacks are caused due to human vulnerabilities and are not at all linked to the password Strength, complexity or recall. This means that the method of password-based authentication in itself, is secure. In fact, it is the simplest yet most powerful authentication method ever invented. The problem, however lies with us, humans. Being emotional creatures, we tend to find easy ways to do things and we tend to fall prey to trickery.

A study has shown that over 50% of IT security staff reuses passwords for workplace accounts. The most common ways of managing work related passwords include remembering passwords using sticky notes, spreadsheets, etc.

Password sharing among employees through insecure mediums is also a common issue observed at many companies. Employees are often seen sharing passwords with each other via phone call, email or sticky notes opening up many avenues for password leaks and resulting into an organization being wide open for a cyberattack.

Let us have a brief look at each type of credential related attacks

### Phishing:

Phishing attacks targeted at stealing the login credentials employ a simple yet effective social engineering technique. Hackers create a webpage that looks exactly same as that of the original for which they are attempting to steal the login credentials. This phishing website is then hosted on a URL which visually looks similar to the original URL (www.facebook.com/www.fabecook.com) a link with this phishing URL is sent to the user via email or message and the unsuspecting user is naturally tricked into entering his/her login credentials on the phishing website.

### Credential Stuffing:

These attacks use advanced computing power available with the cybercriminals to try millions of different combinations of passwords in a very short span of time. Because the strength of a majority of passwords is low along with the high probability that these passwords are not unique, hackers are usually successful in cracking the passwords in a span of a few hours.

### Keylogging:

Keylogging attacks are carried out by installing malware in the user's computer which secretly records the keystrokes and sends it to hackers. Thus, with very little or no effort, hackers succeed in getting access to the user's login credentials. The malware is installed on the users' computer by tricking them into downloading malicious email attachments, visiting malicious websites, Clicking malicious links etc.

Another important aspect of inefficient password management is that of reduced employee productivity. When employees forget passwords for a particular web application, they have to call IT support helpdesk which then helps the employee to reset the password. The process is time consuming and interferes with the employee's workflow thus adversely affecting productivity. A report by Gartner states that the average cost of a password reset to a company is $70 which includes the cost of having a helpdesk for password resets and reduced employee productivity.

All this points us towards a conclusion that there is a strong need for businesses to have a robust password management solution which helps them implement strong password policies so as to safeguard against ever growing threat of cyberattacks while at the same time, overcoming all the inconveniences associated with manual password management.

**Human vulnerabilities have caused losses of approximately $1.8Bn to businesses with an average of $90k loss per business according to the FBI's internet crime report.**

## PASSWORD MANAGEMENT SOLUTIONS

Password managers are pieces of software that allow users to securely store and access all their login credentials in one place. They help overcome the hassle of remembering and manually entering credentials every time users want to login.

Many password management solutions are available in the market today which offer these features. Mostly, these password managers rely on a single master password which the user

has to remember. Upon entering the master password, the users can then access all other passwords stored in their profile. One problem which comes up then is that if the master password is somehow compromised, then all the other credentials stored in the profile become automatically available.

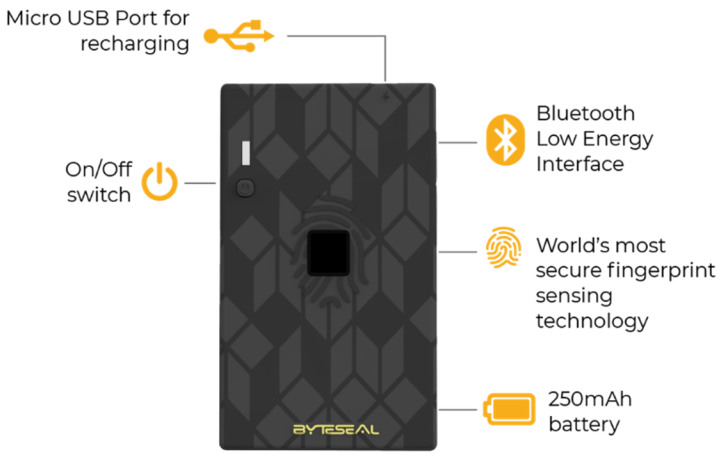
Some password managers enforce multi-factor authentication wherein they either ask the users for OTP which they send to their phone or email, or they ask the users to buy a hardware authentication token and use it along with the master password. While this seems to be a perfectly secure password management solution, the inconvenience which is introduced by the MFA makes it unattractive once more. With MFA, you have to make sure that you always have access to an OTP or hardware token while still memorizing the master password by heart.

An interesting scenario is one where users falling prey to phishing scams and end up giving their master password to the hackers! multi-factor authentication is necessary because humans are gullible even with the master password.

Replacing the master password referred to above with biometrics lets users have their cake and eat it too. It is secure, convenient, and virtually unhackable.

## BIOMTERIC PASSWORD MANAGEMENT

At Byteseal, we have developed a biometric authentication device with a built-in fingeprint sensor and Bluetooth Low Energy 5.0 interface. This device allows use of fingerprint as a



master password. Whenever the user wants to access any of their login credentials stored in the Byteseal vault, they just have to provide their fingerprint on the device and upon successful verification, the login credentials will be autofilled over their respective field on the webpage. The Byteseal Biometric Authenticator enables users to autofill credentials securely with biometrics. It has an inbuilt fingerprint sensor, and works on Bluetooth Low Energy 5.0 interface, making its battery last for weeks! Your fingerprint is your master password. In short, Byteseal provides security of multi-factor authentication and simplicity of first factor authentication

Byteseal's biometric password manager incorporates features like

1. Overall password strength score
2. Import passwords with a .CSV file
3. Share passwords among teams of authorized users
4. Credential Autofill

## SO WHY USE PASSWORDS AT ALL?
## WHY NOT RELY ON BIOMETRICS ALONE?

Password based authentication is widely accepted across all the websites on internet. Very few websites support direct biometric authentication for logins. Migrating to a biometric only authentication is a significant infrastructure change, and hence costly and time consuming. Biometric only authentication is undoubtedly on the horizon, and when we get there, we will all be prepared with Byteseal!

## Contact us to know more

info@byteseal.co

+91-8830697798/902857545

## website

www.byteseal.co