Password Management Software

(Client: Clearfind Technology, 2020)

Introduction

According to Security Magazine, approximately 30 out of 100 remote employees have been hacked since June 2020. Around 50 percent of users use the same passwords for both personal and work accounts, and hackers use this password to access important corporate data. The solution is to develop complex passwords for different sites, consisting of upper and lower case letters, digits, symbols and punctuations.

Password Management software tools not only generate these unique passwords but also store and memorize them, among other capabilities. Enterprises use password managers to keep their accounts secure, provide strong unique passwords for all employee accounts, remove the hassle of resetting forgotten passwords, and save time by auto-filling forms. A growing number of companies use password management tools as their first line of data defense.

What is Password Management Software?

Organizations with many employees often waste valuable time creating and retrieving passwords. Password management software generates and stores strong passwords in a centralized vault - encrypted only with one master password that users need to remember to access their passwords. Additional capabilities vary from one password manager application to another and typically include autofill functionality, checking credentials, providing different types of authentications and sign on preferences, as well as requiring multi-factor authentication information like biometrics.

Password management software has two main components:

(1) Password Generator

The software generates complex passwords for different sites by combining upper- and lower-case letters, numbers, and symbols.

(2) Password Memorization:

The software memorizes and manages passwords by storing them in an encrypted database.

When it comes to storing your password management software, available resources include:

- **Local storage,** where usernames and passwords are encrypted and stored on the user's computer, but are inaccessible on other machines.
- **Cloud-based storage,** where usernames and passwords are stored on a cloud service, enabling users to access their passwords from anywhere.
- **Browser-based encryption,** where usernames and passwords are encrypted in browsers, like Chrome, Firefox, and Internet Explorer.
- **Portable storage,** where usernames and passwords are stored on the users' mobile devices or portable storage devices, such as a USB stick or HDD.
- **Token-based technology,** where users must provide their login credentials and a computer-generated code (or token) for network entry.

Our research shows that within the past six months, the most common use cases for adopting password management software have been:

1. Organizations seeking to improve operational efficiency with protection measures against the rise of hackers.
2. Organizations facing increased security threats as a result of a nationwide shift to remote working, where the security team has limited or no visibility into the applications and tools that employees use.
3. Organizations spurred to boost their IT security by government and industry regulation due to growing global threats.
4. A growing number of employees utilizing convenient password managers on their smartphone or other devices. (The 3rd Annual Global Password Security Report finds

that user retention averaged 30 percent higher after mobile usage was incorporated into a worker's onboarding experience).

The Importance of Password Management Software

- 51% of people use the same passwords for both work and personal accounts[1].
- Stolen and reused credentials are linked to 80 percent of hacking-related breaches.[2]
- Password sharing and reuse remains a common practice in most businesses, with employees reusing one password an average of 13 times.[3]
- Industries with the most sensitive customer data, like insurance and legal, are the least likely to have employees using multi factor authentication.[4]
- 33% of account-compromise victims have stopped doing business with companies and websites that leaked their credentials.[5]
- 37% of internet users say they have to request a password change once a month on at least one website due to forgetfulness.[6]
- Only 45% of US adults change their password for an online account following a data breach.
- 57% of employees find password management a nuisance that stops them from doing their jobs.[7]
- Employees report spending an average of 12.6 minutes per week entering and/or resetting passwords.[8]

---

[1] https://dataprot.net/statistics/password-statistics/
[2] https://www.securelink.com/blog/81-hacking-related-breaches-leverage-compromised-credentials/
[3] https://investor.logmeininc.com/about-us/investors/news/press-release-details/2019/New-LastPass-Research-Finds-Password-Habits-Remain-Key-Obstacle-to-Business-Security/default.aspx
[4] https://www.itsecurityguru.org/2019/10/09/new-lastpass-research-finds-password-habits-remain-key-obstacle-to-business-security/
[5] https://dataprot.net/statistics/password-statistics/
[6] https://cxl.com/blog/password-ux/
[7] https://dataprot.net/statistics/password-statistics/
[8] https://www.businesswire.com/news/home/20190128005147/en/Yubico%E2%80%99s-2019-State-Password-Authentication-Security-Behaviors

Current Landscape

Even before Covid-19, password management software had emerged as an increasingly important cybersecurity tool. A number of factors have influenced its importance.

1. **Growing complex systems & rules for generating and changing passwords**

As the internet grew, websites adopted their own password requirements to deter intruders. Important services introduced extra thresholds on password length and content, with rules that varied between sites. For example, one site required special characters like asterisks or exclamation points in their password, while another site ignored such symbols. The consequences of having so many different passwords augmented the need for efficient password management solutions among enterprises.

2. **The rise of bring your own device (BYOD) & shadow IT**

Bring your own device (BYOD) refers to the trend of employees using personal devices, like smartphones, tablets or USB drives to access corporate data.

As more and more organizations support out-of-office or freelance work, or communicating with the office on work travel or commutes, the threat of shadow IT grew. This is where employees use software or hardware not supported by IT, potentially exposing companies to serious security risks. Password management tools not only make strong passwords enforceable but also gives IT the endpoint control to reduce the risks of shadow IT.

3. **Government regulations**

A Grand View Research market analysis report conducted 2014-2016 found that "increasingly complex compliance, regulatory, and risk management environments in businesses encourage the implementation of password management solutions among industries across the globe."

Data-protection regulations and rules like the 1994 U.S. Federal Computer Crime Act; the 2001 U.S. Computer Fraud and Abuse Act, and the Federal Information Security Management Act of 2002 spurred critical industries, such as healthcare, public sector, and BFSI to adopt password management technology as a security tool for their accounts and devices.

4. **Rise in data breaches**

Companies reported a staggering 4,000 attacks in the last six months alone that exposed personal information such as home addresses and login credentials that could easily be used to steal company data or commit fraud. Not only are people generally lax about security, but there's more information to steal today and hackers have become more sophisticated.

As cyberattacks become progressively more prevalent and far-reaching in their damage, more enterprises seek security tools to protect their data. Password management tools are your first line of account defense.

The Future

The global demand for password management software has witnessed a tremendous rise in the past few years, owing to the emergence of the Internet of Things (IoT), cloud technology, and growing popularity of mobile devices.

As more companies adopt password manager tools, mobile devices are anticipated to become the fastest-growing segment that uses them, according to a 2018 GrandView Market Analysis report.

Features

What to consider when looking for Password Management Software?

Password managers can do a lot more than just generate and save your passwords. We selected the following ten features for best password management tools for your business:

Highly advanced encryption and private adequate security for your passwords - Encryption is the most effective way to achieve data security. The best passwords managers have highly secure tools that sync the saved passwords to the cloud through end-to-end encryption.

Credential Management

Top password managers help you manage your credentials. When you log in to a secure site, the software offers to save your credentials by either storing them locally, on the cloud, as browser-based encryption, encrypting your credentials securely on your device, or giving you the option of accessing them through token technology. The best password managers also help you share credentials with trusted family and friends.

Password Synchronization

Look for a password manager that synchronizes each of your passwords across all your Windows, Mac, Android, and iOS devices. A dedicated password manager allows you to easily access your passwords across all the different computers, smartphones, and tablets you use.

User Management

The best password managers give you the ability to store passwords, user login info and credentials and sync all of it wherever you want across mobile devices and browsers. You can also share a login item with another person.

Single Sign On

A dedicated password manager provides users with the ability to access all applications on their desktop using a single user ID and password.

Biometric

Look for biometric log-in. Such password managers have built-in biometric security systems, where you can set up passwords and sign-in with fingerprint, facial, iris or voice recognition.

Mobile Authentication

Password managers with the most advanced features give you support for biometric authentication on mobile devices too

Out of Band Authentication

Our favorite password managers provide multi-factor authentication, which helps protect you from phishing attempts by requiring an additional form of authorization to log into your accounts, such as a code generated by a mobile app or a fingerprint scan. That's especially essential for the financial sector.

Policy Management

Recommended password managers help managers set up and manage policies like geofencing and IP policies. Geofencing enables you to define parameters of where access is allowed - and where it is not. IP policies help you set guidelines for the consistent and secure management of passwords for employees and system and service accounts.

User Provisioning

A robust password manager allows you to add or remove users to or from a user group. They also manage and edit user information