MARSH

INSIGHTS | JANUARY 2020

Password Managers: Help to Protect Personal and Business Data

Computer passwords do not rank high on anyone's list of favorite things — except for hackers. Most people find passwords hard to remember, too numerous, and an overall nuisance that can distract from their work. But for hackers, passwords provide the ability to pose as authorized users and do damage with relative ease and a low chance of getting detected. In fact, the most common cyber events — phishing attacks — aim mostly at capturing passwords and other login information for systems and accounts. Stolen passwords are a valuable commodity for hackers — almost 70% of hacking incidents involve stolen credentials according to the 2019 Verizon Data Breach Investigations Report.

Despite the availability of login methods such as fingerprint, facial, and voice recognition, passwords remain the bedrock of personal authentication in IT systems today. Because many people reuse passwords across accounts and systems, either directly or with slight modifications, hackers use automated tools to collect them and attempt to use them to access other accounts of that user. This hacking technique, called "credential stuffing", has become one of the dominant methods of account takeover. Users of a number of familiar brands suffered from this type of attack in 2019.

Password management software

Password management software, which is found in modern web browsers and many consumer computing devices, is a common solution that organizes and stores passwords in a single file, and can autofill login information or even automatically enter it on known sites. These tools relieve the user of the need to remember and manually enter login information. Standalone password management apps can also accomplish the same functions.

The password file is normally encrypted and protected by a master password, and in many cases the file is kept in cloud storage to allow access from multiple devices. By doing away with manual entry, password managers effectively negate hackers' ability to use keystroke logging to capture login credentials. Some password managers can create strong random passwords, identify and block the re-use of passwords, refuse to fill forms on phishing sites or insecure sites, alert the user to potential security risks, and advise the user when a password should be changed. Though not without risk, when properly configured and employed, these systems can improve cybersecurity for individuals and help keep them safe online.

Password managers aren't without challenges. Putting all passwords in one file makes that a highly valuable file, the loss or compromise of which could enable a hacker to use or sell all of the user's login credentials. Similarly, if the master password were lost, access to all the protected accounts would also be lost unless an independent secure record of passwords is maintained, which partially defeats the password manager's purpose. Also, a hacker could exploit a bug or an unknown vulnerability in the password manager itself that would put the password file at risk.

SSO: Enterprise-grade password managers for business

Businesses face the same password challenges as individuals, but on a larger scale. With many employees, multiple operating locations, complex policies defining user roles and access privileges, and a multitude of on-premise and cloud-based critical business applications, most businesses need enterprise-grade password management solutions. Such "single sign-on" (SSO) solutions perform the same basic functions available to individuals, but also offer functions that address enterprise needs. Along with encrypted storage of passwords, SSO solutions typically include features such as:

- Integration with enterprise directory services.
- Multi-factor authentication support.
- Attribute-based access control.
- Integrated password policy engines.
- Application programming interfaces for embedding functionality into internally developed business apps.
- Capabilities for unlocking accounts and recovering forgotten passwords.

Other useful features include monitoring and analytics capability, remote device shutdown, and the ability to designate an emergency contact who can access the passwords if the user dies or is incapacitated, without which the accounts and information protected by the passwords would not be accessible.

Recommendations for enterprises

For large enterprises, managing passwords with an SSO solution can enhance the user experience, increase productivity, and improve cybersecurity. It can also make operations more efficient by reducing help-desk support for resetting passwords, which is one of the main tasks that help-desks are asked to perform. Achieving these benefits depends on the solution's effectiveness, implementation, and operational management, but their potential is promising. It is also important that the password manager itself be tested for cyber vulnerabilities and for operational suitability prior to implementation.

Someday we may see the end of passwords. But for today's large enterprise, SSO coupled with multi-factor authentication is a recommended component of a comprehensive identity and access management infrastructure.

Contact:

THOMAS FUHRMAN, MANAGING DIRECTOR
Cybersecurity Consulting and Advisory Services
Marsh Risk Consulting
thomas.fuhrman@marsh.com
+1 703 731 8540

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.