Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Password Managers Usage Recommendations

March 2017

The reference URL for this document: www.m3aawg.org/Password-Managers-BP

Please Note: M³AAWG is presenting the educational information listed here as a service to the industry. However, M³AAWG does not endorse nor recommend any particular password manager solution or provider.

I. Introduction

Password managers have proponents and detractors among users and cybersecurity experts alike. Some insist that usage of a password manager contributes to the application of strong, unique passwords for every online account. To others they represent a single point of failure and are less sure about the value these tools provide. The M³AAWG recommendations presented herein reflect the general consensus of the industry on this subject.

Most users struggle to manage large numbers of usernames and passwords for different websites and other portals that require a login, such as a local computer. Types of reactions include:

- Balking when required to register for yet another account merely to access a report, or make a purchase, and abandoning their efforts
- Reusing the same username and password on multiple sites. This means that if any of those sites are compromised, those credentials must be considered to be compromised at all sites where they have been used previously.
- Picking short or weak passwords, and avoiding long or strong passwords, because using long or strong passwords compounds the problem of having to remember so many distinct online identities.
- Routinely resetting their "forgotten" password each time they visit a site, rather than attempting to remember their username and password.

Clearly, many users have too many unique identities to rely on a good memory alone yet the above typical workarounds are insecure.

II. The Power of Password Managers

The most common answer to this problem is the use of a password manager. A typical password manager provides a number of functions, including:

- Cryptographically-protected, secure password storage (and perhaps secure storage for brief notes, too).
- Tight integration with web browsers (for example, to include auto-filling login forms).

- Generation of complex passwords for use at new sites.
- Offsite back up of user passwords (for example, stored in the "cloud").
- Password synchronization across multiple user devices and services.

Access to the contents of password managers is usually controlled by yet another password that the user must remember. Now, instead of having to remember dozens of passwords or more, users only have to remember a single password; they then have those dozens of secure passwords accessible without having to rely upon an insecure heuristic.

III. M³AAWG Recommendations

- **M³AAWG recommends that most users use a password manager to maintain the majority of their passwords**
- **M³AAWG recommends ISPs and enterprises promote the use of password managers among their users, staff and customers**.

M³AAWG recognizes that some users may have special security concerns, or physical realities, incompatible with the use of a password manager (for example, logging in to a local machine where a user must have their password memorized as the password manager is stored on the machine itself). In such cases, users may need to use an alternative approach more appropriate to their unique requirements.

IV. Conclusion

The recommendations from M³AAWG do not pick technology "winners" and "losers," but accepts that a technology well suited for one environment might be a poor fit in a different environment.

M³AAWG also recognizes that use of a password manager is not without risk. If a password manager becomes compromised, accounts on diverse systems may be impacted.

Some users may have a mix of work or professional passwords, and home or personal passwords. Users may want to keep those credentials separate, either by running a product that supports such a split, or by use of two distinct products, with each of those products reserved for one particular browser.

Even so, M³AAWG strongly recommends that most users use a password manager and encourages ISPs and enterprises to promote the use of password managers among their users, staff or customers.

V. References

1. "Basic security practices regarding passwords and online identities," https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities
2. "Guide to Enterprise Password Management (Draft)," particularly section 4.3, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

3. "Password Managers,"
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_en.pdf

4. "Password Security, Protection, and Management,"
https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf

5. "Review: Best Password Managers for the Enterprise,"
http://www.networkworld.com/article/3011735/security/review-best-password-managers.html

6. "The Best Free Password Managers for 2016,"
http://www.pcmag.com/article2/0,2817,2407168,00.asp

7. "Top Password Managers Compared,"
http://www.csoonline.com/article/2877613/identity-access/top-password-managers-compared.html

8. Wikipedia List of Password Managers
https://en.wikipedia.org/wiki/List_of_password_managers

As with all best practices that we publish, please check the M³AAWG website (www.m3aawg.org) for updates to this document.

M3AAWG110