Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

March 31, 2020
CS-03-2020

PASSWORD MANAGERS

OVERVIEW

People tend to use weak passwords or re-use the same passwords for various online accounts. This increases a person's vulnerability to account compromises stemming from brute force attacks or data breaches, which could then lead to identity theft and other fraud. One way to minimize this risk is by utilizing a password manager. A password manager is a program that can create, store, and manage complex passwords for endless accounts. This not only secures a person's online accounts but also adds a level of convenience by not having to remember or type multiple passwords. The data is typically protected by military grade encryption and a user only needs to remember one master password to access and utilize the passwords stored inside their "vault". However, due to the way many password managers are designed, they also pose some concerns that users should be aware of.

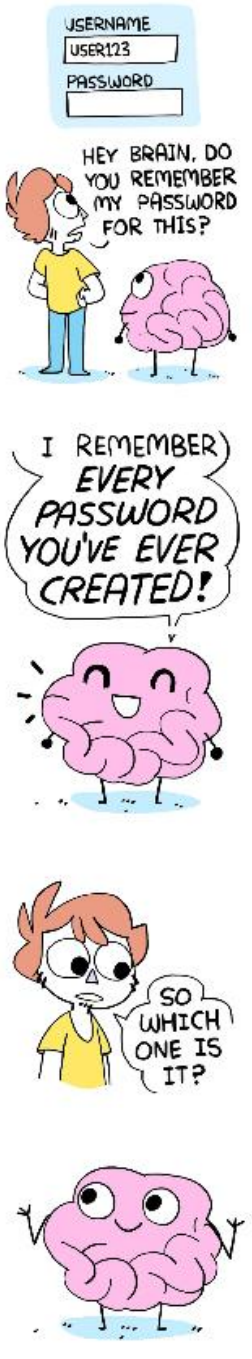

Image Source: instagram.com/shencomix

PASSWORD HYGIENE

To help keep online accounts secure, experts suggest using strong passwords. A strong password avoids common words/phrases, is at least 15 characters long (the longer the better), and contains a random mix of uppercase, lowercase, numbers, and special characters. Alternatively, a passphrase, which is a sentence-like string of random words, can also be used. Passphrases are generally easier to remember while at the same time maintaining or exceeding proper password length. Experts also recommend using a different password for every account, so if a password were to be exposed from a data breach or brute force attack, that same password could not be used to access another account. Unfortunately, due to the vast amount of online accounts a single user has, it has become near impossible to memorize a strong, unique password for every single account. To combat this issue, experts recommend the use of a password manager to help manage and remember passwords.

HOW CAN PASSWORD MANAGERS HELP?

A password manager is a program which uses one master password to manage and store all other passwords for various online accounts. Aside from passwords, users can also save email addresses, usernames, and the websites associated with those passwords. When a user visits a

website, the password manager detects which online service is being accessed and prompts the user for their master password. Once entered, the password manager then displays the available credentials for that website and then populates the credentials into the sign-in form. On top of the convenience provided, this feature also helps prevent users from entering their credentials into a spoofed website meant to phish the user's credentials. Aside from credentials, password managers can also assist with securely storing credit card information, personally identifiable information, and secure notes. This provides the opportunity to store sensitive information encrypted, instead of using an insecure method such as a text-based document, spreadsheet, or note.

Many password managers come with a password generator, which will create randomly generated passwords or passphrases that can be used to secure a user's online accounts. A different randomly generated password (as many characters long as the website allows) should be used for each online account. Additionally, some password managers can check a user's accounts for re-used passwords, credentials exposed in data breaches, and overall password strength.

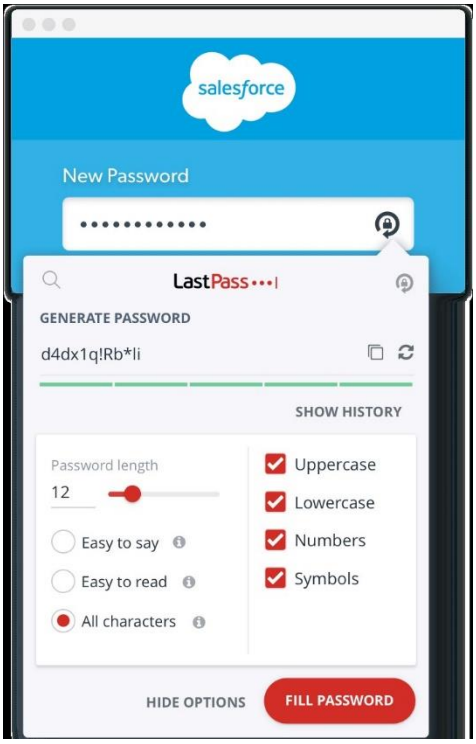

Image Source: lastpass.com

A password manager is most secure when a user's passwords are only stored encrypted on a user's local device. However, many password managers offer encrypted storage of a user's credentials on both a user's device and in the cloud so the user's credentials can sync and be available across multiple devices and via an online portal. When using a password manager that utilizes cloud storage, it is important to ensure that the password manager is practicing "zero-knowledge". With zero-knowledge implemented, the company never knows or stores a user's master password and therefore does not have the key to decrypt the user's data. Even if a password manager's servers were to become compromised, the data would be encrypted with the user's strong, unique master password and therefore render the data useless to the malicious actor.

There are many password managers that are built for and can sync across mobile phones (iOS and Android), computers (Windows, Mac, and Linux), internet browsers, and online portals. Some popular password managers include LastPass, 1Password, Dashlane, KeePass, and Bitwarden. Many offer free versions, as well as paid or premium versions that come with additional features such as; unlimited account entries, unlimited device syncing, family/business plans, password sharing, automatic password reset of compromised accounts, dark web monitoring, encrypted file storage, backups, and various other features. It is

recommended users conduct thorough research on multiple password managers before ultimately settling on the one that best meets their needs.

Web browsers such as Safari, Chrome, Firefox, and Edge have built-in password managers. While these password managers may seem convenient, they are not as secure as a dedicated password manager and lack several of the features mentioned above, and therefore are not recommended.

PASSWORD MANAGER – CONCERNS AND CONSIDERATIONS

While there are many benefits to using a password manager, users must also be aware of the various risks posed by these programs. When using a password manager, all passwords are protected by one master password. While this is good in the sense that only one strong, unique password needs to be remembered, it also means that if a user forgets or loses their master password, they will lose access to all online accounts managed by the password manager. Due to the zero-knowledge concept that many password managers exercise, a password manager company will not be able to reset a user's password. Therefore, it is recommended that the master password is written down and secured in a safe, offline location until it is permanently committed to memory. Additionally, a password manager may provide a user with a recovery phrase/key that can be used in the event of a forgotten/lost password. If provided with this, it is also important to document it and store it in a safe, offline location.

If a user chooses to utilize a password manager that only stores encrypted data locally on their primary device, they could lose access to all their passwords if that device is lost, damaged, or stolen. Because of this, encrypted backups of the data are highly encouraged and should be stored on a separate device in a secure location.

A master password should not be used anywhere else. If this same password is used elsewhere and then exposed in a data breach, a malicious actor could use those same credentials to access a user's password manager account, and subsequently all their passwords. For added security, it is recommended that some form of multi-factor authentication (MFA) be placed on the password manager. Common forms of MFA include receiving a one-time PIN (OTP) code sent via text message or obtaining a OTP code from an authenticator application, such as Authy, Google Authenticator, or Microsoft Authenticator. However, users should be aware that losing access to their device that receives these OTP codes could prevent them from obtaining these codes and subsequently cause them to lose access to their password manager account if MFA is enabled.

Several protections and restrictions on a user's device should be enabled to prevent unauthorized physical access to their password manager. For example, the device housing the password manager application should be encrypted with a strong password. Setting up a PIN code to open the password manager application in place of the master password is not secure or recommended. To make authenticating easier on a phone, most password managers allow a user to utilize facial and fingerprint recognition. Additionally, password managers should not be set to remain unlocked for a set amount of time after entering in the master password, due to the possibility of someone gaining physical access to the phone prior to this time expiring. If a device is ever lost or stolen, several of the above restrictions and protections will prevent unauthorized physical access to the sensitive information stored within the password manager.

Many password managers can also act as an authenticator app to generate MFA codes for accounts stored in the password manager. After populating the credentials for an account requiring MFA, the password manager will automatically copy the OTP code to the clipboard, which will then allow a user to paste it into the input box asking for the code. Although this may sound convenient, this is a great example of "don't put all your eggs in one basket". If a user's password manager were to become compromised, a malicious actor would not only have access to all their passwords, but also the MFA codes needed to gain access to their online accounts. For this reason, it is recommended that MFA codes are managed in a separate authenticator application. Similarly, answers to security questions, recovery codes, and backup codes should be stored in a secure location separate from the password manager.

Lastly, it is important to keep in mind that a password manager is still susceptible to a compromise via malware installed on a device. If the malware contains a keylogger, the master password can easily be captured while it is typed in. Furthermore, once the password manager's vault is unlocked, malware could capture the credentials in the password manager and exfiltrate the data. Therefore, it is important to ensure the device being used is free of malware so a password manager can securely be used.