Everything You Wanted to Know About a Password Manager

Introduction

If you think about it, what is the security protocol which is used the most to access your workstation, wireless device, or even your Smartphone? It is the password. The password has been around for the longest time, and even at one point, presented itself as one of the best forms of security. But today, we are now witnessing its vulnerabilities.

Despite the attempts to fix them, passwords are fast becoming the weakest link in the security chain for any corporation or business. Why is this the case? In today's workplace, employees have to access many types and kinds of resources which are stored on network drives.

Rather than having to create and use a separate password for each and every application, many organizations these days are now allowing for the use of one password to access all of these resources. This is also known as a "Single Sign On" (also known as an "SSO").

As a result, businesses and corporations are making their employees create passwords which are very difficult to remember.

Because of this, there is a strong tendency amongst employees to write their passwords down on a small, sticky sheet of paper known as a "Post It", and attach it to their workstation monitor. But this too becomes a major security problem, because the password is now visible to everybody in the organization.

The solution to all of these vulnerabilities is the use of a Password Manager.

The Password Manager

It can be difficult for an employee to create a password which is complex. Truth be told, creating a new password every few months is the least favorite chore of any worker. When they do create it manually, very little thought is given to it.

As a consequence, corporations and businesses are now turning towards the use of a Password Manager software package (or even a Mobile App) to help not only employees create robust passwords, but to help them remember it as well.

So, what exactly is a Password Manager? It can be defined as a specific application which has been designed to create passwords which are hard to crack, but to also help the end user store and use their passwords more securely. The intent here is to reduce the risk of the password of being a major target for Cyberattacks.

The passwords which are stored in these applications are encrypted. The Password Manager can be stored locally onto the employee's workstation or even in the Cloud, if their employer provides this resource to them. The former can be referred to as "Offline Storage"; and the latter is often known as "Online Storage" (this is discussed in more detail later).

The basic premise of the Password Manager is to give the employee the ability to store all of their passwords into a single repository.

The Corporate Benefits of Using a Password Manager

This application brings in many benefits, which include the following:

1) Only one password is needed:

   In order to unlock and harness the power of your newly deployed Password Manager, you only need to create one master password. But remember, keeping this Master Password secure is up to your employees, the application cannot manage this one component. It can only secure those passwords which actually ***reside within it***.

2) The ability to create very complex passwords:

   Remember, one of the primary goals of a Password Manager is to literally "remember" those passwords which you store into it. You can now create passwords which are complex and difficult enough to crack, so that ***you do not have to remember them***. In order to accomplish this specific task, the Password Manager uses what is known as a "random generator", to create these complex passwords. It does this hard work for your business, so your employees do not have to waste their valuable work time. This also helps to prevent employees from having to write down their passwords on Post It Notes.

3) Using the SSO functionality more securely:

   The concept of this was eluded to in the beginning of this article. The truth of the matter is while that using this approach is very advantageous to a business or a corporation, SSO's are not securely implemented. By using a Password Manager, an SSO can be securely deployed, and in fact, it will even use Cryptographic principles in order to scramble the password so it will be rendered useless, in in the off chance it was to be intercepted by a malicious third party. The end result is that your workforce will be more productive when they access the multiple applications they need easily and securely.

4) It is very easy to change passwords:

   Password resets is not only a drainage of time to the IT staff of a business or a corporation, but it can also be costly as well. For example, it can cost up to $300 per year per employee just to reset these passwords. But by using a Password Manager, your employees can reset their own work related passwords when they need to, without having to call upon the IT staff do that work.

5) You can use the Autofill very easily on Web forms:

   The Password Manager not just stores passwords, but it can also save other personal and work related information of your employees as well. So, depending upon how strict your security policies govern Internet usage, employees do not have to waste time either when filling in one of those time-consuming Web forms (these are often used in those instances of downloading a whitepaper, video, or audio podcast).

6) Access multiple devices:

By using a Password Manager, your employees can also access multiple wireless devices as well (such as using the same password to access a Lenovo brand laptop and an iPhone). This makes it very easy and productive to conduct work related tasks, especially if the employee is a "road warrior", meeting with prospects and customers in different geographic locations. This also helps to reduce the security threats brought by the BYOD ("Bring Your Own Device") trend. This is where an employee uses their own, unsecure wireless device to conduct work related matters.

What You Really Need to Know About Password Managers

Although your business or corporation may now be using a Password Manager, you still need to give extra thought as to how to best use it effectively. There is often the feeling that by utilizing it, everything is all safe and secure. But, this is not completely true either. Password Managers too, just like the Passwords themselves, are also prone to Cyberattacks.

Take these into consideration:

1) Make sure that your Password Manager uses some level of Cryptography:

   In a very broad sense, Cryptography is the science of scrambling information and data while it is in transit, and descrambling it when it reaches its point of destination. Password Managers which make use of Cryptography represent the actual password as "hashes", meaning they are in a garbled state until they are used to access a specific application. Not all Password Managers have this extra functionality, so make sure that yours has this.

2) Offline and Online:

   Password Managers come in either an offline or an online state. With the former, the passwords which are used to access your different devices are not automatically synchronized with another as you update or change you them. This means that you have to move the encrypted database of the Password Manager manually amongst these multiple devices. Or, you could use a Cloud based sharing service like Dropbox to do the synchronization for you. The disadvantage here is that you have to rely upon an extra tool. But, with the latter (online), the Password Manager will automatically synchronize any password changes or updates for you, in just a matter of a few minutes.

3) Make use of 2FA:

   2FA simply stands for "Two Factor Authentication". As it was mentioned earlier, the Master Password which is created is not stored in the Password Manager. Thus, it is the responsibility for your employee to keep it safe. To add an extra layer of security, make sure that your Password Manager makes of the 2FA functionality. This primarily involves using a one-time code which is sent via SMS to your Smartphone, or it could be generated securely with a 3rd party app such as Google Authenticator.

4) Don't forget to log off!

   When we are at work, and logged into multiple applications, there is a tendency to forget to log off when we are done using them. Obviously, this does carry inherent security risks with it.

Therefore, when you are not using your Password Manager, make sure you log off immediately. Many Password Managers of today will also automatically log you off after a short period of inactivity. Make sure that you have this functionality enabled.

Conclusions

As businesses and corporations are becoming security conscience and making employees create complex passwords, the need for using a Password Manager becomes even greater. Workers have enough job tasks to accomplish, and having to create passwords just takes extra time out of their day.

Let's face it, every time we get that pop up message on our workstation to create a new password, we cringe at the thought of having to come up with something new.

Using a Password Manager will greatly eliminate all of these administrative headaches, and will also help to make sure that employees stay focused on their work-related responsibilities. One of the greatest assets that a Password Manager brings to the table is that it will alert you in real time when your password appears to have been hacked, or compromised.

Without using such a tool, we never know when our password has been hacked into, until it is too late (like the recent Yahoo security breach).

Also, if you choose to create a new or updated password from within the Password Manager, it will alert you as to whether your newly created password is strong or weak, by using either a number or color scale.

For example, the number 1 could indicate a very weak password, and the number 10 could represent the strongest password possible. This could also be represented by the colors red and green, respectively.

Remember, the Password Manager is so far one the best ways to make sure that we all stay safe on the Internet!!!

Sources

https://www.rit.edu/security/content/benefits-using-password-manager

http://www.pcworld.com/article/3085395/security/5-things-you-should-know-about-password-managers.html

http://configurationconnection.com/how-a-password-manager-can-increase-your-productivity/

https://keepersecurity.com/business.html