SECURITY
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

SEC-GDL-019 – Password Managers

Author:	Paul Ferrier
Date:	02/05/2017
Document Security Level:	**PUBLIC**
Document Version:	1.0
Document Ref:	SEC-GDL-019
Document Link:	
Review Date:	May 2018

Document Control							
Version	Author	Position	Details	Date/Time	Approved by	Position	Date/Time
1.0	Paul Ferrier	Enterprise Security Architect	Prepared the document for publication	02/05/2017			

Table of Contents

SEC-GDL-019 – Password Managers

Purpose

This document aims to provide information surrounding Password Managers, while it doesn't advocate which product to use, it considers the use of such a piece of software and the benefits that it provides.

Authentication overview

Authentication is critical to ensure the right person has access to the right information thus protecting the confidentiality of the data. For instance, you wouldn't want everyone to have access to your online banking information.

Authentication can be performed in a number of ways with the most common form being that of a username or email address and password. Other forms include biometrics (finger print or retina scanning), security tokens (such as one time access code generators), while they increase security, they also increase the costs to implement (hardware) and maintain (support services for end users) the service.

Unique passwords

In order to protect your information online, it is advisable to use a unique password for each site that you use and this ***really* should not be** your University account password. If this account were to be compromised, you are not only providing the access you have to University systems including your email account, but also to stored information on any shopping site (for example) that you use.

Herein lies a problem, how easy would it be to remember one hundred different passwords for all of the services that you use throughout a year? The answer is very difficult if the passwords are secure (using a combination of upper case and lower case letters, numbers and symbols).

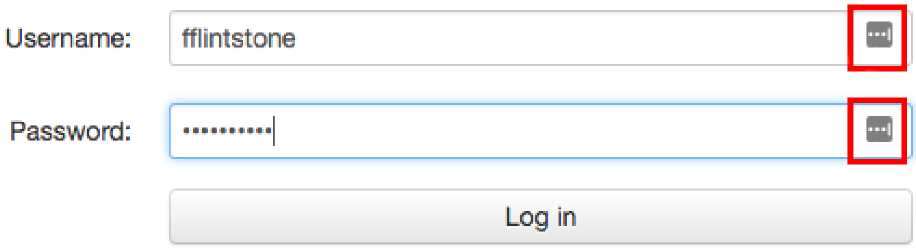
How does a password manager work?

A password manager is a database of sites or services and the associated credentials to be able to access them. They are stored encrypted and protected by one ***master*** password, *this should not be stored in the password manager itself*. You are required to provide this one password to access the entire vault, so rather than remembering one hundred you just need to remember one really secure password.

	Email Address / Username	**Password**
webmail.plymouth.ac.uk	fred.flintstone@plymouth.ac.uk	@7Yz4qiQeQ
dle.plymouth.ac.uk	fred.flintstone@plymouth.ac.uk	@7Yz4qiQeQ
www.bbc.co.uk	fflintstone	5lw8U@Xs2#
Home internet router	fflintstone	a06!F9Vu^Q
Online laundry service	fflintstone17	8^4ZxtRxiq
Supermarket delivery	freddy_flintst	f22Ed!WlFd

As University credentials are stored (for the DLE and Office365) separately, but both services are provided behind the University's Single Sign On mechanism the same information is presented more than once.

When credentials are supplied, they can then be accessed via plug-ins to your Internet browsers (highlighted in the picture on the next page) and when a site or service is accessed, the password manager will either supply and submit the details or auto-populate them and allow you to submit the information.



Username: fflintstone

Password: ••••••••••

Which password manager to choose?

As mentioned earlier, these guidelines will not suggest what should be used, rather it will point to resources for you to consider the benefits for yourself.

http://www.techradar.com/news/software/applications/the-best-password-manager-1325845 (covers the free market)

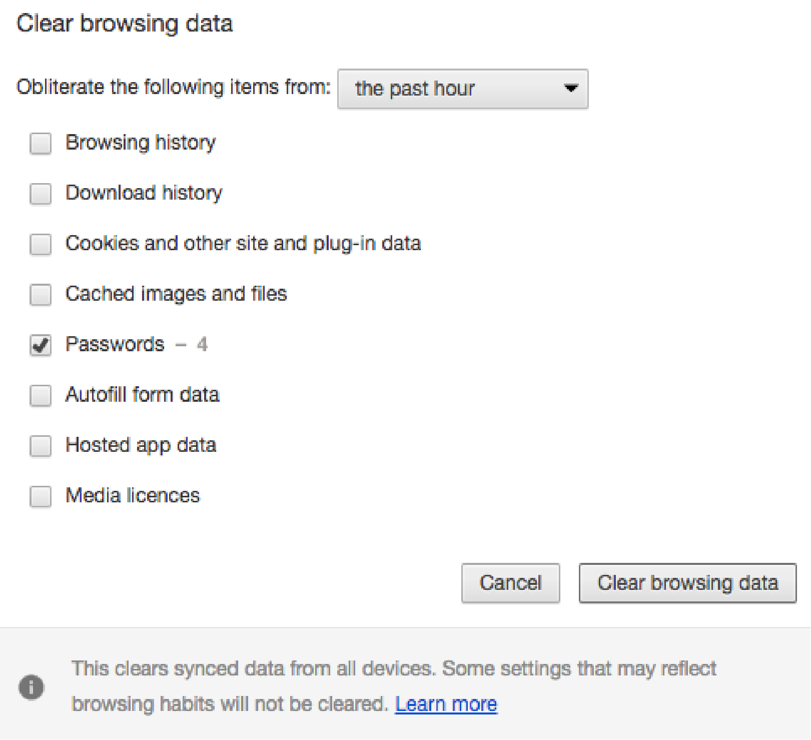
http://uk.pcmag.com/password-managers-products/4296/guide/the-best-password-managers-of-2017 (considers the paid-for market only)

http://lifehacker.com/5529133/five-best-password-managers (a few years old now, but still relevant)

Conclusion

As with all security options, there are freebies and paid-for solutions. The former generally provides the options required for day to day use whereas the latter will provide cross-platform (for use on different operating systems and devices) capabilities and other beneficial options.

Look around and find a solution that meets your requirements, start adding your passwords in o the manager and remove any passwords that are stored in your Internet browsers (as illustrated below from Google Chrome).



Clear browsing data

Obliterate the following items from: the past hour

- □ Browsing history
- □ Download history
- □ Cookies and other site and plug-in data
- □ Cached images and files
- ☑ Passwords – 4
- □ Autofill form data
- □ Hosted app data
- □ Media licences

This clears synced data from all devices. Some settings that may reflect browsing habits will not be cleared. Learn more

Please remember though all of your passwords are now only as safe as your master password – so ensure that this is protected.