Table of Contents

Purpose ........................................................................................................................................... 3
  Authentication overview .................................................................................................................. 3
  Unique passwords .......................................................................................................................... 3

How does a password manager work? .......................................................................................... 3

Which password manager to choose? ............................................................................................. 4

Conclusion ........................................................................................................................................ 4
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.

<table>
<thead>
<tr>
<th></th>
<th>Email Address / Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>webmail.plymouth.ac.uk</td>
<td><a href="mailto:fred.flintstone@plymouth.ac.uk">fred.flintstone@plymouth.ac.uk</a></td>
<td>@7Yz4qiQeQ</td>
</tr>
<tr>
<td>dle.plymouth.ac.uk</td>
<td><a href="mailto:fred.flintstone@plymouth.ac.uk">fred.flintstone@plymouth.ac.uk</a></td>
<td>@7Yz4qiQeQ</td>
</tr>
<tr>
<td><a href="http://www.bbc.co.uk">www.bbc.co.uk</a></td>
<td>fflintstone</td>
<td>Slw8U@Xs2#</td>
</tr>
<tr>
<td>Home internet router</td>
<td>fflintstone</td>
<td>a06lF9Vu^Q</td>
</tr>
<tr>
<td>Online laundry service</td>
<td>fflintstone17</td>
<td>8^4ZxtRxiq</td>
</tr>
<tr>
<td>Supermarket delivery</td>
<td>freddy_flintst</td>
<td>f22EdlWlfD</td>
</tr>
</tbody>
</table>

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.
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://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 into the manager and remove any passwords that are stored in your Internet browsers (as illustrated below from Google Chrome).

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