Simplified Password Management

Introduction

Target Audience

It's an unavoidable necessity in your *digital lifetime* to create accounts and passwords for numerous online systems. The problem this document seeks to address is the flawed approach of using a single password for all online accounts, which is universally recognised as very bad practice. If this is something you find yourself doing, this document may be for YOU. The objective here is NOT to give idealistic advice which reads like the contents of a spy novel, the goal is "good enough security", i.e. something which is fit for purpose.

The Risks of Using a Single Password

In 2016 it was reported that up to 500 million Yahoo email password records had been hacked. If you had a Yahoo account and used the same password for Barclays, Facebook & Amazon, etc. it would have presented a security risk to you far beyond the scope of your Yahoo email account.

Use Different Passwords

It's essential to have different passwords for each and every one of your online accounts. When using identical passwords, your online security is only as strong as the weakest link. You won't know which web site might be vulnerable to hackers, so you need to play it by safe by having different passwords everywhere.

Recommendations

Plan Ahead

Whenever practical, establish (and record) account information and passwords before you reach the stage of creating an online account. This way you avoid the potentially fraught time when you're on your computer or mobile device and a web site is awaiting input.

Password Complexity

Each online system for which you need an account may have different rules regarding the type of characters required in a password. To make it likely that your chosen password will be universally accepted, it's good practice to include the following character types. Uppercase (e.g. **A** or **B**), lowercase (e.g. **c** or **d**), numbers and special characters (e.g. ***** or **$** or **%**). It's sensible to avoid the following: dictionary words, alphabetic sequences and numeric sequences. Plan on using a password length of ten to fifteen characters for every account, but make a single exception for your email account. This account typically becomes the mechanism for you to perform password resets, so make it three characters longer.

Put Similar Characters Together

It's generally convenient to cluster (group) each type of character together to make password entry easier when you're using mobile devices. For example, you could start by putting your numbers together, then your special characters, followed by your lowercase letters before finishing with your uppercase letters.

Make Records of Your Passwords

Using different passwords for all of your online accounts means that you must make proper records, as it's unrealistic to memorize more than a small number of passwords. The **"Magic Number"** section on the following page describes an approach which enables you to securely record passwords in written form. However, if you're comfortable with word processors and spreadsheets, it may be that you can do away with written records altogether. In this circumstance, you're urged to:

a) Save the document with a name which doesn't reveal its contents, i.e. not Passwords.doc

b) Maintain a backup copy, such as a paper printout or digital photo on your mobile phone

The Magic Number

For every recorded password, it's suggested that you insert a character which isn't actually part of the online password. To demonstrate the magic number, **7** is used in the following example as the magic number. When establishing a password, you could write down the following: 49**7**33$cfxpJ. When you enter the password online, the number **7** will not be part of the password - the real password is: **4933$cfxpJ**

Where the number **7** is placed in your recorded password doesn't matter, you could write any of the following:

74933$cfxpJ, 4933**7**$cfxpJ, 49**7**33$cfxpJ.

Recording Passwords

1) Create a table with column names as shown below in a paper based notebook, or use an application such as a spreadsheet or word processor on your computer / mobile device
2) Record new passwords in a row in the table for the new account which you'll create. In the example below, there's a row (record) for Barclays Bank; the real (online) password is: **4933$cfxpJ**

Organisation	Web Site	Account Name	Password	Notes
Barclays Bank	www.barclays.co.uk	janedoe1@yahoo.co.uk	49**7**33$cfxpJ	Blah, blah

Example Completed Table

The example below shows how a password table appears when it contains several records. If the notebook / spreadsheet containing the table of passwords was lost or stolen, the recorded passwords are of no practical use. The number **7** appears obvious in the given examples - this is deliberate, as it's been emphasised by using a red font and emboldened.

Note: The right column shows that the number 7 doesn't appear obvious when it's not emphasised.

Organisation	Web Site	Account Name	Password - Bold	Password - Normal
Barclays Bank	www.barclays.co.uk	janedoe1@yahoo.co.uk	49**7**33$cfxpJ	49733$cfxpJ
Google Gmail	www.gmail.com	janedoe@gmail.com	**7**846akbvkL%	7846akbvkL%
Amazon	www.amazon.co.uk	janedoe@gmail.com	kratoA83**7**J£	kratoA837J£
eBay	www.ebay.co.uk	janedoe12	tm%**7**443DKAR	tm%7443DKAR
BBC	www.bbc.co.uk	janedoeBBC	6**7**34AD%kbfk	6734AD%kbfk
Facebook	www.facebook.com	janedoe@gmail.com	dad%92**7**34F	dad%92734F

Because the table will become essential to you, it's crucial that you have a backup copy of it. For tables in a paper based notebook this can be achieved by taking a photo of it on your mobile phone or scanning it into your computer. For digital tables (created on your computer or mobile device) you could print the document out or save it onto a USB storage device.

Further Password Ideas

- You might wish to use two or more magic numbers, e.g. **365**. In this instance your recorded password would contain a sprinkling of **3**s and or **6**s and or **5**s. Furthermore, you could use a *magic letter* instead of a magic number, e.g. the letter **P**. If you really wanted to impress yourself, you could use a mix of letters and numbers. An example for dog lovers would be to use *canine* - that's the letter **K** and the number **9** 😊 It's most important that you find a balance between complexity and usability that works for YOU.
- You may have heard about protecting your account with two-factor authentication (2FA). This approach relies upon something in addition to your password, such as receiving a code on your mobile phone. If you feel capable of utilising this approach it's certainly to be encouraged.
- There are applications called password managers and web sites which provide the same capability. Password managers enable you to store passwords for your various accounts in a specially protected file on your digital device or an online database. Password management in this way is certainly recognised as very good practice, and their use is strongly encouraged if you feel you can tackle the challenge. I like to think of the magic number approach of using obscured written / typed records as being a stepping stone towards the undoubtedly better solution of password managers.

Addendum

If you already have a system which you are comfortable with for managing passwords, please ignore this document. The magic number approach doesn't claim to be best practice, but it's certainly better than not having a planned and consistent approach.

Please read through these three pages again from start to finish – you'll almost certainly need a second read for the content to fully sink in.