

Simplified Password Management

Introduction

Target Audience

Many people who are not technology savvy, nevertheless find it an unavoidable necessity 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 is NOT to give idealistic advice, the goal is “enough security.” Fit for purpose is the goal, not something you’d likely read in a spy novel!

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.

Use Different Passwords

It’s essential to have different passwords for each and every one of your online accounts. Using the same password for all of your accounts, while simplifying your online experience, MUST be avoided.

Recommendations

Plan Ahead

Whenever possible, establish (and record) account information and passwords before you reach the stage of creating an online account. This approach is far more suitable than 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 (e.g. **elephant**), alphabetic sequences (e.g. **jkl**) and numeric sequences (e.g. **678**). Plan on using a password length of ten to fifteen characters for every account. A single exception is your email account, as this naturally becomes a critical account for you. Because your email is often used for password resets, make it three or more characters longer.

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 following “magic number” section 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 a digital photo on your mobile phone

The Magic Number

For every password which you record, it’s suggested that you insert a character which isn’t actually part of the online password you’ll setup. By way of example, **7** is used here as the magic number. When establishing a password, you could write down the following: **b77J\$49xpy14**. When you enter the password online, the number **7** will not be part of the password - the real password is: **bj\$49xpy14**

The number of **7**s used doesn't matter - you could use one, two or even three instances of **7** in your recorded password. Similarly, where the number **7** is placed in your recorded password doesn't matter, you could write any of the following: **b77J\$49xpy14**, **bj\$49xpy147**, **b77J\$497xpy14**, **b7J\$497xpy147**.

Recording Passwords

- 1) Create a table with column names as shown below in a notebook - or use a suitable application, such as a spreadsheet or word processor
- 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 NatWest Bank; the real (online) password is: **AcJ\$4f9xp33**

Organisation	Web Site	Account Name	Password
NatWest Bank	www.natwest.co.uk	janedoe1@yahoo.co.uk	Ac 77 J\$4f9xp33

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 has been emphasised with a large font and emboldened.

Note: The right column is shown solely for demonstration purposes, real passwords are never recorded here.

Organisation	Web Site	Account Name	Password	Real Password
NatWest Bank	www.natwest.co.uk	janedoe1@yahoo.co.uk	Ac 77 J\$4f9xp33	AcJ\$4f9xp33
Barclays Bank	www.barclays.co.uk	janedoe12	J 7 Ad%86f56n	JAd%86f56n
Google Gmail	www.gmail.com	janedoe@gmail.com	84k 77 L% 7 6akbv	84kL%6akbv
Amazon	www.amazon.co.uk	janedoe@gmail.com	kraA83J 77 £to	kraA83J£to
eBay	www.ebay.co.uk	janedoe@gmail.com	tm 7 % 7 443DKAR	tm%443DKAR
BBC	www.bbc.co.uk	janedoeBBC	63A 77 Dk4b% 7 fk	63ADk4b%fk
Facebook	www.facebook.com	janedoe@gmail.com	d92 7 34% 7 adF	d9234%PadF

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

To manage inevitable password ageing changes, it can help to leave space after the recorded password in the table. This approach enables you to simply add characters such as X, then B, then 4, etc., rather than the commonplace replacement of a 1 with a 2, then with a 3, etc.

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 **3s** and / or **6s** and / or **5s**. 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 with a similar function. While being recognised as good practice approaches for the computer literate, they're beyond the scope of this document.

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 two pages again from start to finish - you will almost certainly need a second read for the content to fully sink in.