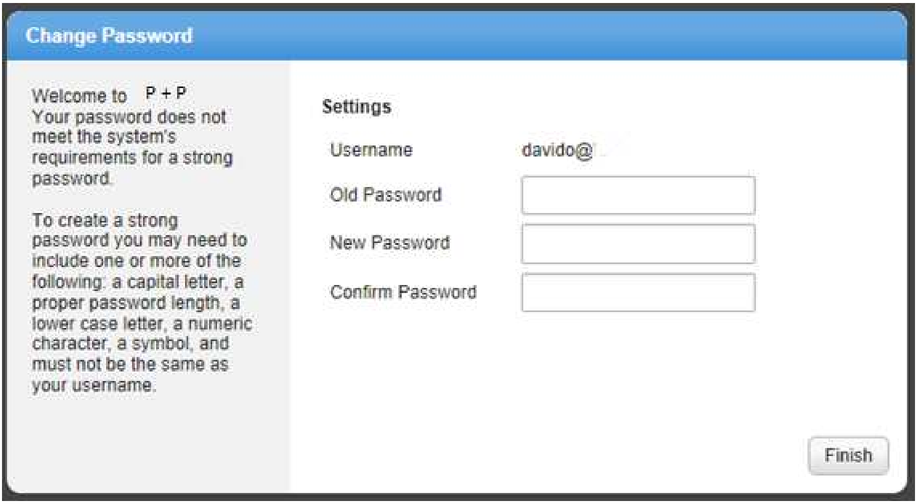
Performance Plus ™
Partnership
Enabling Business Excellence



Change Password

Welcome to P + P
Your password does not meet the system's requirements for a strong password.

To create a strong password you may need to include one or more of the following: a capital letter, a proper password length, a lower case letter, a numeric character, a symbol, and must not be the same as your username.

Settings

Username davido@

Old Password

New Password

Confirm Password

A Simple Guide to a Practical, Pragmatic, Personal Password Policy

Practical – Straightforward, easy to use
Pragmatic – Not perfect (because nothing ever is) but useable
Personal – Because it is personal to you
Password – The key to safe use of on-line sites
Policy – A set of rules that you can follow to make your life easier

WARNING – READ THIS FIRST!
It's just possible that you are one of the few people in the world who are incredibly well organised and who - when faced with a demand from yet another on-line site that requires you to enter a 'strong' password that is different from all your other on-line passwords - consults their personal password policy and enters that unique, strong password.

If you are that person then don't bother reading the rest of this guide; take pity on one of the (far greater) number of disorganised souls who go completely mind-blank at that type of request and give this guide to them – they really need it!

Contents

©Performance Plus Partnership 2017 – all rights reserved
PerformancePlus Document Ref PPP002/2017 Issue #1
Author David Baker

Introduction

You have presumably acquired this little guide either because you have realised that you have a need for a Practical, Pragmatic, Personal Password Policy or possibly some smug, self-satisfied individual who thinks that they know everything about everything has decided, on your behalf, that you fit this criterion and has given it to you – either way, I hope you find it useful.

The concept behind this guide is…

When you are faced with the next on-line site that, before it will let you partake of its wonderful, glittering content, demands that you enter a password that is both unique (i.e. is not the same one that you use for all of the other on-line sites that you subscribe to) and contains all the requirements of a very strong password (i.e. it contains both upper and lower case letters, numbers and non-alphanumeric symbols and is at least eight characters in length)

…it ensures you will have a simple set of rules to follow that will provide you with a strong and unique password which (and this is the really good bit!) will enable you to easily recall that password when you next need to access the site.

A few words of warning though - If you follow this guide when setting your on-line passwords, it's roughly the equivalent of fitting a good quality, 5-lever lock to the front door of your house. It doesn't make your house burglar proof; it doesn't stop people getting in if you don't lock the door and it definitely doesn't stop them getting in if you give them a copy of your key! What it does do is to make it reasonably safe and secure from casual intruders, provide a delay to the accomplished burglar that would probably make them choose another victim and, most importantly, allows you easy access to your property (providing that you don't lose the important key).

Step 1 – Choose a few ‘Very Strong’ core passwords

These core passwords will (as the name defines) form the core of your Personal Password Policy (PPP).

How many is ‘a few’? Well, this rather depends upon how many you can easily remember and how many on-line accounts you have (or are likely to acquire) but a minimum of four is probably about right.

What’s the definition of ‘Very Strong’? Basically a very strong password should consist of a minimum of eight characters – but more is better and ten to twelve is about right – and there should be a mix of alphabetic characters in both upper and lower case, some numbers and, ideally some non-alphanumeric symbols (such as $, % or #).

If you want to get a simple measure of how good your chosen password is then there are a number of on-line password strength calculators that you can use to check your choice – I tend to use http://www.passwordmeter.com/ as it gives you both a percentage figure and individual suggestions as to how you could improve your choice but there are lots of others out there.

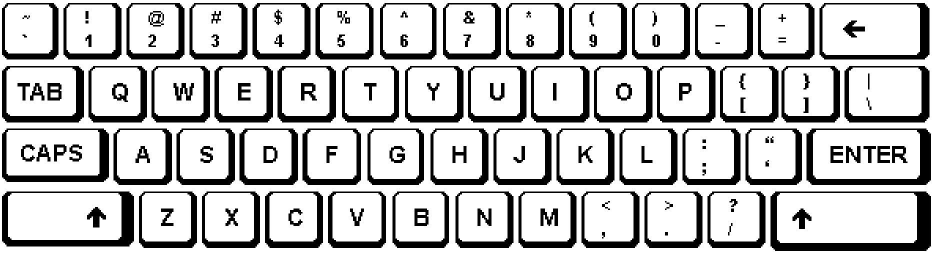
Now you could choose a random selection of letters, numbers and symbols (and, again, there are plenty of on-line, random password generators out there) but personally I find it really hard to remember random passwords so the suggestion is that you use a password strategy – and I’m going to suggest two possible strategies that you could use.

Core Password Strategy 1 – Transposition

You've probably heard of the German Enigma cipher machine from the Second World War (and if you haven't there are loads of good books and films about it that you really should look at). The Enigma machine looked like a primitive typewriter and, essentially, provided a pseudo-random but repeatable letter transposition for its operators i.e. they pressed one letter and the machine returned a second, different letter. What I'm suggesting here is a far simpler technique using a standard PC keyboard.

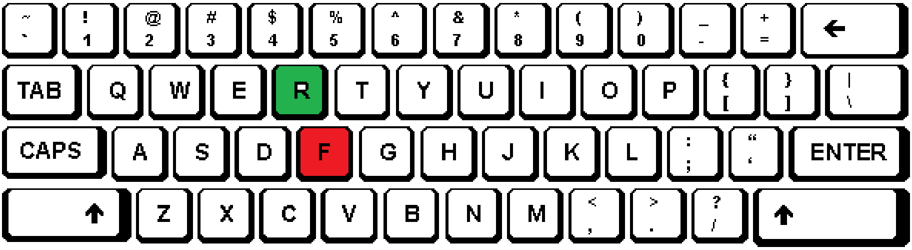
First of all choose a word that is meaningful for you and is around 8 to 10 characters in length. For example, let's say your town of birth is Felixstowe in Suffolk and use that.

A standard PC keyboard looks something like this:


~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = ←
TAB Q W E R T Y U I O P { [}] | \
CAPS A S D F G H J K L : ; " ' ENTER
↑ Z X C V B N M < , > . ? / ↑

Now choose a basic strategy which, for example, might be "Above and Left"

On that basis the capital “F” in Felixstowe is transposed to a Capital “R” see the Red and Green letters below (because “R” is above and to the left of “F” – get it?)



Now use the same strategy to transpose the rest of the letters of your chosen word and Felixstowe then becomes R3o8sw5923 (which Password Meter rates as 100% even though it doesn’t contain any symbols)

You could equally use a strategy of “Above and Right” in which case Felixstowe would transpose to T4p9de6034 – it doesn’t really matter what strategy you choose as long as you remember it yourself.

The potential problem with this strategy is if you are using a phone, tablet or some form of virtual keyboard which does not match the layout shown above because, more often than not, the numeric and symbol keys are on a separate screen. This does not prevent you using some form of transposition strategy, it just means that it will not generate numbers and symbols automatically. If you look at the next suggested strategy you can see that this issue can also be overcome fairly easily.

Core Password Strategy 2 – The Pass Phrase

Generally speaking, people remember phrases far better than words so possibly you have some well remembered phrases you could use to generate your core passwords.

For example, if you are of a religious persuasion you might well have a prayer or religious phrase that sticks in your mind – for Christians, the first line of the Lord's Prayer might be one:

Our Father who art in Heaven hallowed be Thy name

Now take the first letter of each word in the phrase:

OFwaiHhbTn

Now that's a good start but if you check it in Password Meter it only rates as "Weak 42%" which is really not good enough. However Password Meter also suggests that it would improve if you added some numbers and symbols so changing the "O" of "Our" to "0" (the number 0) and the "i" of "in" to a "1" and adding an exclamation mark at the end changes it to:

0Fwa1HhbTn!

Password Meter rates this as "Very Strong 94%" which is far better – it does however mean that you have to remember to change the letters into numbers and add the exclamation mark.

Another example might be a simple nursery rhyme such as:

Jack and Jill went up the hill to fetch a pail of water

Now take the first letter of each word in the phrase (and use "&" for "and" and "2" for "to")

J&Jwuth2fapow

Password Meter rates this as "Very Strong 91%" which is very good

Final note: You could use either or both of the above strategies or you could devise a completely different one of your own – the important bit is that you actually have a strategy (or strategies) and that you remember what it is!

Step 2 – Assign clues or nicknames to your core passwords

Taking the examples above:

The clue or nickname for **R3o8sw5923** could be **“Town above left”**

The clue or nickname for **0Fwa1Hhbtn!** could be **“Prayer by numbers!”**

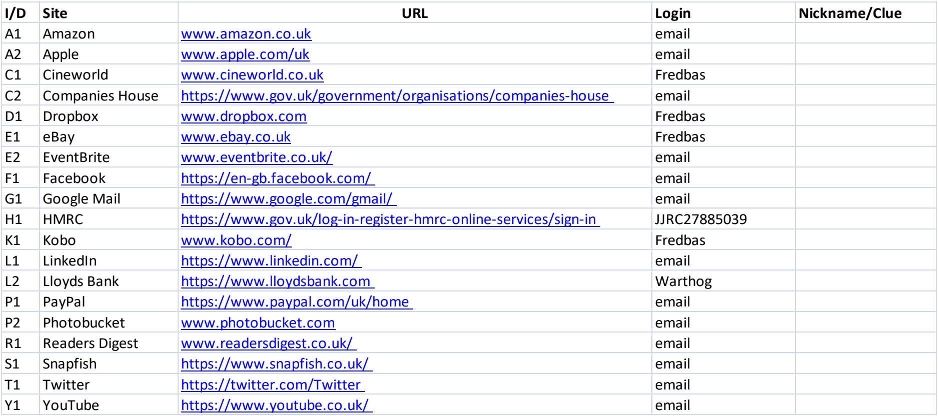
The clue or nickname for **J&Jwuth2fapow** could be **“Nursery rhyme”**

The point here is that your clue must remind you of your chosen word or phrase and, preferably, your chosen strategy.

Step 3 – Make an alphabetically sorted list of your on-line accounts

You can do this any way you like but, personally, I would suggest using a spreadsheet like Microsoft Excel (it's really not complicated so you don't need to be a spreadsheet genius but it does make it look nice and neat and it's easy to edit).

In the words of one well known TV chef – "here's one I made earlier".



I/D	Site	URL	Login	Nickname/Clue
A1	Amazon	www.amazon.co.uk	email	
A2	Apple	www.apple.com/uk	email	
C1	Cineworld	www.cineworld.co.uk	Fredbas	
C2	Companies House	https://www.gov.uk/government/organisations/companies-house	email	
D1	Dropbox	www.dropbox.com	Fredbas	
E1	eBay	www.ebay.co.uk	Fredbas	
E2	EventBrite	www.eventbrite.co.uk/	email	
F1	Facebook	https://en-gb.facebook.com/	email	
G1	Google Mail	https://www.google.com/gmail/	email	
H1	HMRC	https://www.gov.uk/log-in-register-hmrc-online-services/sign-in	JJRC27885039	
K1	Kobo	www.kobo.com/	Fredbas	
L1	LinkedIn	https://www.linkedin.com/	email	
L2	Lloyds Bank	https://www.lloydsbank.com	Warthog	
P1	PayPal	https://www.paypal.com/uk/home	email	
P2	Photobucket	www.photobucket.com	email	
R1	Readers Digest	www.readersdigest.co.uk/	email	
S1	Snapfish	https://www.snapfish.co.uk/	email	
T1	Twitter	https://twitter.com/Twitter	email	
Y1	YouTube	https://www.youtube.co.uk/	email	

Some notes on the spreadsheet:

1. The I/D is a row or line number with the letter of the alphabet for that or those entries (i.e. A for Amazon and Apple) and if you need to add another account, for example ao.com then it would go in as A3 (which of course Is not strict alphabetic order but at least the first letter is right!)
2. The Site column is for the name that you use for that site
3. The Login for many sites is more often than not your email address (hence putting email here) but, for some it is different

Step 4 – Now assign password clues or nicknames to your list

Here it is again with nicknames

I/D	Site	URL	Login	Nickname/Clue
A1	Amazon	www.amazon.co.uk	email	Town Above Left
A2	Apple	www.apple.com/uk	email	Town Above Left
C1	Cineworld	www.cineworld.co.uk	Fredbas	Nursery Rhyme
C2	Companies House	https://www.gov.uk/government/organisations/companies-house	email	Town Above Left
D1	Dropbox	www.dropbox.com	Fredbas	Nursery Rhyme
E1	eBay	www.ebay.co.uk	Fredbas	Nursery Rhyme
E2	EventBrite	www.eventbrite.co.uk/	email	Prayer by Numbers!
F1	Facebook	https://en-gb.facebook.com/	email	Prayer by Numbers!
G1	Google Mail	https://www.google.com/gmail/	email	Town Above Left
H1	HMRC	https://www.gov.uk/log-in-register-hmrc-online-services/sign-in	JJRC27885039	Prayer by Numbers!
K1	Kobo	www.kobo.com/	Fredbas	Nursery Rhyme
L1	LinkedIn	https://www.linkedin.com/	email	Town Above Left
L2	Lloyds Bank	https://www.lloydsbank.com	Warthog	Prayer by Numbers!
P1	PayPal	https://www.paypal.com/uk/home	email	Prayer by Numbers!
P2	Photobucket	www.photobucket.com	email	Nursery Rhyme
R1	Readers Digest	www.readersdigest.co.uk/	email	Nursery Rhyme
S1	Snapfish	https://www.snapfish.co.uk/	email	Nursery Rhyme
T1	Twitter	https://twitter.com/Twitter	email	Town Above Left
Y1	YouTube	https://www.youtube.co.uk/	email	Prayer by Numbers!

Step 5 – Understand how to make a site password

A site password comprises the I/D number combined with the core password

For example the Lloyds Bank site password will be L2 combined with Prayer by Numbers! or:

L20Fwa1Hhbtn!

This, incidentally, improves the password strength to “Very Strong 100%”

Step 6 – Update all your on-line site passwords and double check that you have entered them correctly

Step 7 – Now make multiple copies of your list

If you’ve created your password list in a spreadsheet program then I would definitely keep a copy on your computer in this format (that way you can edit it and add to it as required) but there’s nothing to stop you printing a copy or two to leave where you can find them easily.

The beauty of this system is that it really doesn’t matter if other people look at your password list provided that you never tell them your strategy or strategies and your core passwords or phrases.

What you might want to do is to keep a note of those core passwords and strategies in some very secure place well away from your computer (with your solicitor or in a safe deposit box or something similar) so that if you should get eaten by a lion or run over by a number 10 bus then the executors of your will can get into your on-line accounts and delete them.

But what if…

This is the section you arrive at when, for some reason, your carefully constructed PPP doesn’t work on one or more on-line sites. The potential reasons for this are numerous but include:

- The site only accepts a maximum of 8 characters
- The site doesn’t accept non alphanumeric symbols
- The site demands that you change the password on a regular basis (and won’t let you repeat a previously used password)

Many of these objections can be handled by choosing another core password that is both shorter and doesn’t generate any non alphanumeric symbols. For example choose **Monkey** as your memorable word and use an Above Left transposition to generate **J9hi36** – now add the I/D for the site and it becomes something like **X1J9hi36** if the site name starts with an “X” (which is still a “Very Strong 86%” rating).

Your nickname/clue for this core password could be something like **“Cheeky”**

If you have one or more sites that demand a regular password change then just add another column to your spreadsheet which gives the date of the current password e.g. 1216 for December 2016 and then add that to the site password.

The list then looks something like this:

I/D	Site	URL	Login	Nickname/Clue	Date
A1	Amazon	www.amazon.co.uk	email	Town Above Left	
A2	Apple	www.apple.com/uk	email	Town Above Left	
C1	Cineworld	www.cineworld.co.uk	Fredbas	Nursery Rhyme	
C2	Companies House	https://www.gov.uk/government/organisations/companies-house	email	Town Above Left	
D1	Dropbox	www.dropbox.com	Fredbas	Nursery Rhyme	
E1	eBay	www.ebay.co.uk	Fredbas	Nursery Rhyme	
E2	EventBrite	www.eventbrite.co.uk/	email	Prayer by Numbers!	
F1	Facebook	https://en-gb.facebook.com/	email	Prayer by Numbers!	
G1	Google Mail	https://www.google.com/gmail/	email	Town Above Left	
H1	HMRC	https://www.gov.uk/log-in-register-hmrc-online-services/sign-in	JJRC27885039	Prayer by Numbers!	
K1	Kobo	www.kobo.com/	Fredbas	Nursery Rhyme	
L1	LinkedIn	https://www.linkedin.com/	email	Town Above Left	
L2	Lloyds Bank	https://www.lloydsbank.com	Warthog	Prayer by Numbers!	1216
P1	PayPal	https://www.paypal.com/uk/home	email	Prayer by Numbers!	
P2	Photobucket	www.photobucket.com	email	Nursery Rhyme	
R1	Readers Digest	www.readersdigest.co.uk/	email	Nursery Rhyme	
S1	Snapfish	https://www.snapfish.co.uk/	email	Nursery Rhyme	
T1	Twitter	https://twitter.com/Twitter	email	Town Above Left	
X1	Xenon	www.xenon-services.co.uk/	email	Cheeky	
Y1	YouTube	https://www.youtube.co.uk/	email	Prayer by Numbers!	

…and the site password for Lloyds bank from December 2016 until the next requested change would become:

L20Fwa1Hhbtn!1216

(And just in case you are wondering or thinking that I might be giving some of my details away, I will state that while all of the above sites exist and some of them I do actually have accounts with, none of the account passwords are ones that I use)

A Final Word (or two)

As I said in the introduction, adopting a Personal Password Policy does not convey total protection to your online activities in the same way that fitting a 5-lever lock to the front door of your house doesn't make it burglar proof. What it does do is to make you think a bit more about your online security, encourage you to use unique and strong passwords for all the sites that you visit and gives you an easy way to remember that strong password when you next visit a site.

Another point concerns so-called security questions that some sites require you to enter in addition to your password. In most cases, the reason for asking the security question is to allow the site operator to tell the user what their password is (or to reset that password) on the occasion when the user has forgotten what they set their password to. The questions often take the form of asking you to enter things like:

- Your mother's maiden name
- Your town of birth
- Your first car

The points to remember here are that:

- You don't have to tell the truth (even if your Mummy told you that you always should)
- No one is going to check what you answered
- Your answer doesn't have to make sense (to anyone but you)

Look at it in another way and suppose that someone was trying to break into your on-line bank account. It would be relatively easy for them to find out your mother's maiden name (if you'll excuse the pun) and your town of birth; depending on your age it wouldn't be too difficult to guess what your first car was (the Ford Fiesta was probably the most popular first car for a certain generation). But if you have chosen a strategy such as keyboard transposition for your passwords, then use that to answer the question or questions e.g.

- Mother's maiden name = **Baines** but transpose it to **Gq8h3w**
- Town of birth = **Slough** but transpose it to **Wo97ty**
- First car = **Fiesta** but transpose it to **R83w5q**

It doesn't matter what your strategy is as long as you remember it and you stick to it

Some Other Dangers

It’s tempting isn’t it, when that extremely helpful Internet browser software that you are using to access all those exciting on-line sites, offers to store your login and password details for the next time that you visit that site for which you have just entered a very strong password? But should you do so?

The security professional in me wants to scream “No, don’t do it” but the pragmatic (for which in this case read lazy) part of me says “Provided that you are the only person using that computer (phone, tablet, whatever…) and you have set some form of locked access to it when you are away from it then it’s an acceptable risk”. If, however, it’s not your personal computer and especially if it’s a shared device in an Internet Coffee Shop for example then definitely don’t do it.

That leads nicely into whether you should use public Wi-Fi connections on your laptop, tablet or phone to access sites that require you to enter a login and password – especially things like internet banking sites or company intranet sites. The clear and unequivocal answer to that is “ABSOLUTELY NOT” unless you are using a secure VPN or virtual private network. Doing this is roughly equivalent to handing your front door key to a burglar and saying “look after that for me will you as I’m just off on holiday for a month”!

And if you don’t know what a VPN is then it’s about time that you found out.

PerformancePlus and how we can help you

At PerformancePlus we help our business clients to create and maintain practical policies and management framework systems that are both comprehensive in relation to the relevant international standards and yet are easy to operate and that not only help them to achieve standards certification, if they require it, but also enable them to run their businesses more efficiently and more effectively.

We help businesses obtain international standards certification in the following areas:

Quality – ISO9001

Environment – ISO14001

Data & Information Security – ISO27001

Health & Safety – OHSAS18001

Whether you require some initial consultancy, a gap analysis (to tell you what needs to be done to achieve certification), internal or external auditing, ongoing support or just some basic advice, we can help you.

And best of all, our charges are extremely reasonable and the initial visit to assess your requirements is free

Contact us on 01284 330 400 or sales @performanceplus.co.uk

PerformancePlus™
Partnership
Enabling Business Excellence