PASSWORD PROTECTION

By Sarah Wischmeyer, May 2018

FORM OVER FUNCTION

Effective passwords must be very long (**at least 14 characters!**) and **unpredictable**. Equally important, we should **never reuse passwords** – so we need a unique password for every digital portal we access.

Added measures such as incorporating special characters or regularly changing our passwords help a bit, but they tend to add more complexity for the human than the decrypting machine. Truly it's the **(1) length, (2) novelty, and (3) single-use of passwords that make them effective**.

THE CHALLENGE IS OBVIOUS

How can we remember so many passwords? How can we even think up so many passwords? How do we remember which password goes where? How do we manage changing passwords?

There are other challenges too. Are our secret questions very secret? Do our personal devices reveal our secrets?

BE PROACTIVE

We might not answer every security threat, but we can make some simple changes to our passwords that move us substantially in the right direction.

EFFECTIVE PASSWORDS

Here's a good trick for creating memorable yet **"very strong"** passwords: use a **phrase**, then **vary it** in a novel way. And to create several effective passwords: use a **theme**. For example:

- **Dates:** `IWasBorn@112288!` *OR* `WeMoved@DC2007!`
- **Quotations:** `ToBeOrNotToBe@HamA3S1!` *OR* `2BOrNot?@DaneHamlet`
- **Titles:** `Pride&Pred#5Daughters` *OR* `DieHard3#Bruce&Sam`
- **States & Fruits & Animals:** `LA$Limes&Lions` *OR* `PA$Peaches&Pandas`

These examples are rather simple. You can add complexity to your pattern and theme by including another category, using initials, avoiding repetition, etc. Keep in mind, the variance really ought to be creative – that is, unpredictive to a machine that uses algorithms based on common patterns like "123" etc.

NOTE: There are Password Managers that generate random strings of words, though I prefer to create my own phrase because it's easier to remember something that is personally meaningful, and it's easier to remember multiple passwords that are connected by a theme.

As for those "secret questions," keep in mind that you don't have to give an answer that matches the question, nor a simple answer. For example:

- **Q:** What is your mother's maiden name? **A:** `MamaMia!` *OR* `NoneOfYourBusiness`
- **Q:** What was the name of your first pet? **A:** `San Diego Zoo` *OR* `Topeka KA pet`
- **Q:** Where did you go to high school? **A:** `Space Camp` *OR* `Topeka KA school`

Portals & Email

Next, consider all the places where you use passwords. Obviously, you will want to use very strong passwords for sites that access your financial and health records. But also, it is very important to **secure your primary email** accounts because if you "forgot your password" you will use your email to reset your password as well as receive email alerts if your password has been changed.

Hey, you can have more than one email address! By doing so, you can **relegate one or two addresses** to less secure portals such as social-media or shopper-rewards sites. You don't even need to check these emails accounts. But if you do want the content – e.g., you want your reward coupons – then you can set up your smart phone or Outlook / Mail to pull in all the relevant email addresses you do use. Even so, having all that marketing email funnel to a separate account improves both security and organization!

It is extremely important to **use a different password for each** web portal and email address! If a system is breached (e.g., Facebook, Twitter, Equifax, etc.), you will be ever so happy that the criminals did not get the password to your bank account. You will be happy too that you don't need to change a compromised password in 20 other places. By the way, use unique answers for your **secret questions too**!

The Master List

O.K. So you now have several emails and passwords. How do you remember them all? Ultimately, you will need to **write it down**. You can keep the master list in a Password Manager, a file on your desktop computer, a rolodex, etc.

You could also use a **private shorthand code** and prompts to further encrypt the list. For example:

- `LA$Limes&Lions` could be written: `LA $ Lim & Lio`
- `PA$Peaches&Pandas` could be written: `PA P**ch**&P*nd**`

But Not Here

Don't let your browser remember your password! And it's best to keep the full Master List **off of portable devices** that you use in public.

Secure Devices

I truly believe that the companies providing our hardware, software, and cloud services do strive to deliver secure products and systems, in part because these companies are betting their future profitability on our willingness to trust them with our content. That said, I also believe there will always be security threats and risks that we can mitigate with good practices, beginning with these steps:

- Use anti-virus software and firewalls, and stay current with updates
- Use two-factor / multi-factor authentication methods
- Seek continual education on how to avoid phishing scams and other hacks
- Be mindful of vulnerable networks such as public "free" Wi-Fi or even Bluetooth
- Use passwords that are at least 14 characters, random, and never reused