How to manage and remember your online passwords
David McLelland - Technology and Online Security Expert

Whether it's our email, social networks, telephone or electricity bills, online auction sites or online banking, we're all being asked to keep track of an increasing number of passwords and pin-codes to secure our access to services online.

According to research by credit reference agency Experian on average we each have 26 online logins, with 25-34-year-olds managing 40 online logins each. Those figures were from 2012 - they're likely to have risen further since then.

How do we manage all of these passwords?

Password management is a central part of staying safe online, but recommendations to never to use the same password more than once are difficult to make practical when we have so many different online accounts. Experian also found that even though we might have 26 different accounts on average, we only used 5 different passwords!

Why should we use different passwords for each of our online accounts?

Imagine you are shopping for a Father's Day gift online, you find something you really like but have to create an account so you can order it - annoying, right? But very common. You have to create a username and password, so you use your email address and your usual password because they're easy to remember. You're also asked for your address plus your place of birth or mother's maiden name for extra security or in case you forget your login details.

Your father's day gift gets delivered, everybody's happy, you forget about the account you just created. Unfortunately that online retailer gets compromised and the usernames and passwords of everybody who has shopped there fall into the hands of online criminals.

Sounds unlikely?

Thinking “that will never happen to me”? It’s more common than you might think...

- Yahoo
- Dropbox
- Evernote
- Tumblr
- Spotify
- eBay
- Kickstarter
- LinkedIn
- PlayStation Network

Each of these services has experienced a high-profile security breach over the last few years, possibly exposing your sensitive information to online fraudsters.

And the scary thing is, these are just the ones that we know about - who heard of the Heartbleed Bug that was all over the news earlier this year? This high-profile security vulnerability was around for well over a year and affected two thirds of all websites before its discovery was made public; but that’s not to say that hackers didn’t know about it long before.

So, back to our Father’s Day Gift story

The hackers have a list of usernames and passwords. Your username, as you remember, is your email address, so immediately they can start sending phishing emails and other spam to your account.

Is the password you provided when you created your account is your usual one, the same one you use for most of your online accounts? Including your email account? So the fraudster can now log in to your email account, take control of it by changing the password and locking you out, and then start sending spam to your contacts and sifting through your emails for something they can use to make money. The identity theft isn’t yet complete as the fraudster might also try your PayPal account, your Facebook account - simple if they all use the same username and password.

So, that’s the reason why we should never use the same username and password across different online accounts

It’s like having a single key that unlocks your car, your front door, your windows and your safe. If somebody gets hold of that key, they’ve got access to everything.

Top Tips for Tough Passwords

If that's not difficult enough, we need to make sure that the passwords we do use are as secure as they can be so they can't be guessed or 'brute-forced' by hackers (where the hacker will try every common word in the dictionary as a password - and with some software they might be able to do that in a matter of seconds). So:

- Don't use names of family members, place names - any information that people trying to guess you password might easily be able to find through your social network page or official registers.

- Don't use normal dictionary words - try replacing numbers with letters or with punctuation, so a 3 instead of an E or 4 instead of an A, perhaps an exclamation mark instead of a 1.

- Try using just the first letters of a memorable word or a phrase or song that means something to you, replacing some of those letters with numbers and punctuation.

- There are free services online that tell you how secure your password is - be sure to use a credible one like the Microsoft Password Checker (https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx)

Some online services and sites now let you use something called **two-factor authentication**. So, your online banking might ask you for the password and PIN that you've remembered but also some digits from a separate card reader or dongle; or if you're logging on to a service from a new computer for the first time you'll need not only your password but a passcode that gets sent to your mobile phone as a text message. The idea is that your password by itself, should it get compromised, won't be enough to gain access to your account.

Password Management Tools

So, you've got a secure password that will be very difficult for an online fraudster to guess or brute-force, but the problem still remains that you've dozens of accounts that you need to remember. That's where a **password management tool** comes in.

Password Management Tools remember your passwords for you, enter them into your web browser for you, they can even create new passwords automatically to save you the trouble. Many synchronise across multiple devices, be it your tablet, smartphone or PC. Best of all, they do it very securely.

There are a handful of well-known ones - including:

- LastPass
- KeePass
- Roboform
- Dashlane
- 1Password

- Norton Identity Safe
- F-Secure Key

Some are free, some cost literally a few pounds, but they can save you plenty of time and hassle of remembering dozens of passwords, and give you peace of mind.

Storing all of your passwords in a single place may seem like a bad idea, but used properly it's far safer than using the same password across all of your services or trying to remember your passwords individually by writing them down.

Assume your account will be compromised

The thing is, even if we keep our side of the bargain by maintaining secure online passwords, the online services themselves are increasingly the targets of malicious attacks, and have been found wanting when it comes to security.

So, perhaps it's safest to assume that - at some point - one or more of our accounts might be compromised. And, were that to happen, what would the damage be? What privileged information would a hacker have access to?

Maiden names, places of birth, pets' names – all of these are common security questions but they can often be discovered by fraudsters from social networking sites, public records or social engineering. There are more ways to lie than to tell the truth, so be creative!