Four steps to a simpler, safer password system

June 3 2014, by Andrew Smith

What do you mean 'IHATECAT' is not a strong password? Credit: konsvi, CC BY-NC-SA

Several high-profile security breaches have, of late, got many people wondering about their passwords.

It would be great news if I could tell you a perfect sure-fire system to manage your passwords; the reality is that you have to make your own

choices. Many of us struggle to remember one password, let alone many, so changing passwords often makes life a little difficult. But if, like many others, you feel like it's time to start again, there are ways of doing it right. Think of it as your new password ecosystem.

1. Rank your accounts

Step one of your new password system involves grouping the different online accounts you have according to their importance. You should rank your accounts according to the importance of the activities you carry out on the different sites.

Social media accounts, for example, might have a ranking of one, and cloud services such as dropbox or iCloud, a rank of two. Sites on which you make purchases, for example Amazon or eBay, are more important, and would have a ranking of three.

Next comes email, which is too often overlooked. These accounts are far more enticing for cyber-criminals than your Amazon account since they are often the gateway to many other accounts so they should be given a ranking of four.

And finally, online banking and Paypal should carry a ranking of five.

Once you've decided your ranking, you can set login names and passwords. All should be equally complex but you can treat some passwords as less important than others.

Sites with a ranking of one could easily share the same login email, but have different passwords. Whereas ranks four and five must be different.

2. Don't overlook your username

You've got your ranking and are ready to start, we tend to focus our concerns on passwords but your username is another important piece to the puzzle. We all often use similar usernames to access our multiple accounts. It could be a secret name, such as fluffybunnykins, or more often it is your email address.

If I know your personal email address, I know too much. This was how a hacker calling themselves Oleg Pliss recently compromised iPhones. This attack did not involve infiltrating iPhones, instead it involved finding out email addresses from other sites and applying that information to take control of phones.

If your email-based login has been used on one site that has been compromised and you are using the same password somewhere else, there is the outside possibility that these other accounts may also be exploited.

It's not practical to maintain an email address for every online account but multiple email accounts are advisable. Look back at your ranking and try to use a different email address for the different ranks. You can easily attach your email software to multiple email accounts. So, in reality, this does not make life too difficult.

3. The tricky bit

The biggest challenge for most people as they begin their new password life will be to pick passwords that are complex enough not to be compromised but easy enough to remember.

Start by thinking of a meaningless word. It should be something that

someone else couldn't guess so children, pets, football teams and hometowns are a bit of a giveaway. It is worth taking a moment to think of something that you can only ever recall.

You do need to make sure that your word is at least ten characters in length. The reason that we like longer passwords, is that it takes brute force crackers more time to break them.

Now you get to make it obscure, the more you can use capital letters, numbers or symbols (such as *&%$@) the better. Different sites do have different policies so try using one of each and already your password is harder to guess. Even if I now know what your meaningless word is, I still do not know how you have obscured it.

Let's say your chosen password is the meaningless word "timecheese". From this word you could create TimeCheese, t1meChee5e or T1meCh_e5e. There are many combinations. You can test out different passwords for strength on dedicated sites and even use a random word generator if you are struggling with ideas.

4. Remembering your password

Now you have created your meaningless word, apply some common sense. Will you actually remember it? Passwords like DarkCalamariSandwich fit the criteria for length and nonsense factor. But there are a lot of characters to remember and possibly too many options for adding in numbers. A week after setting it, will you remember whether you replaced the i with a 1 or the s with a 5?

You need to create something that is relatively simple by using random words that you connect together. Typically I would suggest two words to most mortal souls, but some people will remember more.

Often word associations help. You might use "Dr Who Cheddar" as a prompt to recall timecheese. While you should obviously never write down your password, there's nothing wrong with making a note of the association to jog your memory. If timecheese was your eBay password, you could write down "auction tom baker cheddar". A Dr Who fan might see the connection but they still probably wouldn't be able to work out the actual password.

These steps should help you start a new password life but you still need to change your passwords regularly, particularly when breaches like those seen over the past few weeks happen. You are the only person who can really protect your information online.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation