Tip Sheet

Creating strong, safe passwords

Ensuring the security of multiple online accounts might seem like a big task, but it is important you do not use the same password for all of your accounts. Data breaches of well-known websites are becoming more common, and using the same password across multiple accounts puts you at risk of cyber-criminals accessing your banking, social media accounts and other personal information.

Here are some tips for creating strong, unique passwords that will keep your personal information safe online:

DO

- Use long passwords – they are harder to crack. Aim for eight or more characters.
- Use variety – the greater variety of characters in your password, the better. A strong password will include a combination of lower and upper case letters, a special character (for example: $, #, *), and a number.
- Change your passwords regularly – set an automatic reminder to change them every few months.

DON'T

- Use the same password for more than one account – if hackers are able to obtain your online password for one account, they can run software to try the same email/password combination for all your other accounts.
- Use common words that can be found in any English or foreign dictionary.
- Use words spelled backwards, common misspellings or abbreviations – for example: *koolpassword* or *retupmoc*.
- Use sequences or repeated characters – for example: *123ABC* or *qwerty.*
- Use any of your personal information – for example do not use your name, yours or your family's birthdays, your street name or your passport number.

Some creative solutions to keeping track of all your passwords

Create a short phrase that you are likely to remember. For example, *John Smith will make 30 cakes on Friday*. Now, simply take the first character from each word to create your password, where the example would become *JSwm30coF*. Notice how there is a mixture of upper case, lower case, numerals, and just to be sure, you can put a special character at the end, to create a strong password like: *JSwm30coF*.*

Another example, *Alex Harris can eat 10 hot dogs only on Thursdays*, will become *AHce10hdooT*. Once again, adding a random, special character will add to the strength of your password, so this password becomes: *#AHce10hdooT*. These types of passwords are extremely strong, as they are very long and do not use common English words.

You could also consider using password-management software. Depending on which software you choose, the basic idea is that the software will generate and manage your passwords for all your sites across all your devices. Some examples include LastPass, RoboForm Pro or Sticky Password. But make sure that any password-management site you use is secure by reading their privacy policy.