Every time we go online we have a risk to be tricked by hackers and let them fetch our personal information or even identity. They use different tricks and approaches for sniffing our information they can use for illegal actions.

Created a good password? You need to do more than that!

It is very important to understand what it is not enough to have a good password to keep our data secure. First, we have to be very careful and be mistrustful every time we need to provide or share our information. There are some main tips on protecting us from the main threats are listed below, have a quick look and consider the suggestions before we move to a “How to make a good password?” section.

* Dispose old devices securely. Use utility programs to completely wipe a storage. Deleting our personal information from the hard drive is not enough as some of the data still possible to retrieve. Remove external memory card and a SIM card from an old device.
* Use a good and efficient security software to protect a computer and make sure it is always up-to-date.
* Our phone is like wallet. Just imagine how many personal information is stored on our phone. Put a pin, password or a pattern on your device to protect yourself from unauthorised access.
* Be extra careful — Make sure you are using only trustful websites and services, be aware on email scams and do not open unexpected and suspicious emails.
* Never provide your sensitive information if someone is asking for it by phone, email or in any other way. Instead, be mistrustful, find a company’s phone number on an official website, give a call and double check if they really need that information.
* Do not over-share your information. Your passwords can be guessed by scanning information you are posting online on blogs or social networks. Never give obvious answers on the security questions if you are asked to provide them during a registration with any of the services or accounts.

How to make a good password?

* Never use any information related to you in a password (names, birthdates, pets, addresses, phone numbers etc.). Do not use dictionary words or meaningful combinations of dictionary words for your passwords. For example, “watermelon” or “sweet watermelon” are bad passwords.
* The use of numbers, symbols and a mix of uppercase and lowercase letters will make a password much harder to guess as the amount of possible combinations will be much bigger.
* The longer the password, the harder it is to guess. Use at least 8-12 digits for a password.
* Never use the same passwords across different accounts and services. If someone get your password for one of the accounts, that person will be able to gain access to your other accounts.
* Do not share a password with anyone else. For example, friends may become ex-friends or a person you are sharing your password with can be not as careful as you are and use the password on an unsecure machine.

Well, that’s good to have a strong password, but how to memorise it?

It is difficult to remember multiple passwords for different accounts. A trusted password manager is a good solution. Let them securely store your passwords and memorise a password just for that service. Spend some time checking out the reviews and reputations of available password managers.

Here are a some of the top ones to start with:

* Lastpass
* Roboform
* Kaspersky Password manager

Do not want to trust your passwords to anyone?

There are some ideas on how to make a memorable strong password and here is a most popular.

It easy to remember a sentence like “The first mobile phone I had was Nokia 3200, I paid 150 pounds for it.” Take first digits and then turn that into a password, so your password would become “**TfmpIhwN3200,Ip150£fi”.** This is a strong enough password consisting of 21 digits.