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.

It is very important to understand what it is not enough to have a good password to keep our data secure, we need to do more than that. 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?

**don’t use the same ones across different accounts.**

Use a different password for each of your important accounts, like your email and online banking accounts. Re-using passwords is risky. If someone figures out your password for one account, that person could potentially gain access to your email, address, and even your money.

Using numbers, symbols and mix of upper and lower case letters in your password makes it harder for someone to guess your password. For example, an eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 times as many possible combinations than an eight-character password with only lower case letters.

Create a unique password that's unrelated to your personal information and uses a combination of letters, numbers, and symbols. For example, you can select a random word or phrase and insert letters and numbers into the beginning, middle, and end to make it extra difficult to guess (such as "sPo0kyh@ll0w3En"). Don’t use simple words or phrases like "password" or "letmein," keyboard patterns such as "qwerty" or "qazwsx," or sequential patterns such as "abcd1234" which make your password easier to guess.

**The longer the password, the harder it is to crack.**

Stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they’re obvious, is also bad. For example, “house” is a terrible password. “Red house” is also very bad.

For example, maybe you can find it easy to remember a sentence like “The first house I ever lived in was 613 Fake Street. Rent was $400 per month.” You can then turn that into a password by using the first digits of each word, so your password would become **TfhIeliw613FS.Rw$4pm.**This is a strong password at 21 digits.

Do not share with anyone, friends – ex-friends, not that careful and use on a not secure machine.

If you have a difficult time remembering multiple passwords, a trusted password manager may be a good solution. Spend a few minutes checking out the reviews and reputations of these services.

Lastpass

Roboform

Kaspersky Password manager