

Интернет е уникален инструмент за учене, откриване на информация, играене на игри, споделяне и гледане на забавни клипчета!

Но също така трябва и да си наясно какво да правиш онлайн, за да защитиш себе си от всеки, който може да те разстрои, нарани или да открадне от теб.

Ако вече правиш всичко необходимо, за да си в безопасност в Интернет, тогава помогни на друга нинджа, също да се защити!

ПАРОЛА

Слагай винаги силни пароли, които можеш да запомниш и пази паролите в тайна и на сигурно място.

Твоята парола е като ключ за сейф или за къща – много по-лесно е да проникнеш вътре с ключ, отколкото без такъв!

Повечето сайтове имат правила за дължината на паролата, раличните букви и цифри, които трябва да се използват и пр. , но е хубаво винаги да следваш няколко основни правила:

1. По-дългите пароли са по-сигурни. Избирай пароли с поне 10 знака.
2. Избягвай използването на името на сайта или на твоето потребителско име в паролата. Избягвай също така имена и рождени дати на членове на твоето семейство.
3. На колкото по-малко места използваш определена парола, толкова по-добре – така дори и някой да я научи, ще успее да влезе само на няколко места.
4. Паролата на основния ти имейл не бива да бъде парола никъде другаде! Ако някой успее да влезе в пощата ти, може да смени всичките ти останали пароли!
5. Можеш да използваш мениджър за пароли, които ще ти позволи да имаш и съхраняваш много дълги и сигурни пароли. Но не забравяй, че трябва да помниш паролата на самия мениджър за пароли!

Също така, някои сайтове предоставят възможност да те разпознаят по два начина – парола и потвърждение на код през телефония ти номер – така дори някой да е разбрал паролата ти, не може влезе в профила ти, ако няма телефона ти.



С подкрепата на:



СПОДЕЛЯНЕ И СОЦИАЛНИ МРЕЖИ

Трябва да внимаваш, когато споделяш информация, видео или снимки онлайн, които биха могли да се използват, за да те намерят, наранят, притеснят или разстроят - сега или в бъдеще.

Винаги се питай:

1. Може ли тази информация да бъде използвана, за да открият къде се намирам в момента, къде живея или кое е училище уча?
2. Човекът, с когото споделям, виждал ли съм го лично лице в лице?
3. Човекът, с когото споделям, макар и да познавам лично, използва ли нов профил, който никога не ми е споменавал, че има?
4. Може ли това, което споделям, да ме злепостави или нарани сега или в бъдеще?

Ако отговорът, на който и да е от тези въпроси, е „ДА“, тогава не споделяй!

Трябва да си сигурен, че във всяка социална мрежа настройките ти за поверителност са каквито е необходимо, за да си защитен, и ги проверявай редовно! Твоят родител/настойник може да ти помогне да го направиш.

ВИРУСИ И ЗЛОВРЕДЕН СОФТУЕР

Компютърът ти може да бъде заразен от опасен софтуер от посещението на заразени сайтове или от свалянето на заразени файлове, игри, видеа и др.

Можеш да се защитиш по два начина:

- 1) Винаги внимавай какви сайтове в Интернет посещаваш и какво сваляш!
- 2) Винаги имай инсталирана и активна антивирусна програма на компютъра си (Avast е добър вариант за безплатна антивирусна програма).

ИЗИГРАЙ СВОЯТА РОЛЯ

Ти самият също си от значение, за да може Интернет да е по-добро и по-сигурно място за другите хора!

Не обиждай и не тормози другите - това не е готино. Бъди съпричастен и добър с всички.

НО НЕ ЗАБРАВЯЙ: Ако някога се притесниш или разстроиш от нещо, което си видял, направил или някой е казал за теб или за някой друг, винаги споделяй възрастен, на когото имаш доверие!

С подкрепата на:

