ПРАВИЛА ЗА БЕЗОПАСНОТО И БЕЗПРОБЛЕМНО СЪРФИРАНЕ

ПРАВИЛА, КОИТО ЩЕ ПОМОГНАТ ЗА БЕЗОПАСНОТО И БЕЗПРОБЛЕМНО СЪРФИРАНЕ НА ВСЕКИ УЧЕНИК В ОНЛАЙН ПРОСТРАНСТВОТО.

Ето ги и тях:

1. Използвай сигурна парола за профилите си

Употребата на силна и защитена парола е от изключително значение за безопасното ти присъствие в интернет. Препоръчително е тя да съдържа поне 12 символа и да се състои от комбинация от малки и главни букви, цифри, символи и др. Също така да не присъства в правописния речник, да не съдържа лични данни (име, телефон, рождена дата) и да не е създадена с предвидими „трикове“ *(пример: h0use)*.

Сменяй паролата си редовно, не я използвай на няколко места и най-важното – не я записвай никъде и не я споделяй с друг, защото може да попадне в ръцете на злонамерен човек. Силните пароли са трудни за помнене, но от голямо значение.

Ако искаш да тестваш комбинации и да провериш колко са сигурни те, ти предлагаме да го направиш **тук**. Имайте предвид, че паролата трябва да е измислена, а не актуална на някой от наличните ти профили.

2. Прави редовно архивно копие на информацията си (backup)

Колкото и надеждно да изглежда твоят компютър, той в никакъв случай не е защитен срещу повреди и вируси на 100%. Като поддържаш актуално копие на архивираните ти данни, няма защо да се притесняваш за изгубена информация, независимо от това в какво състояние е устройството ти (било то телефон или лаптоп). Това помага и в случай на загуба или кражба на устройството ти, когато обикновено най-лошото е загубената заедно с него ценна информация.

Архивирането на данни звучи като досадна, сложна и времеемка задача, но всъщност има много услуги, които го предлагат (до някакъв обем и безплатно). Не е сложно, отнема малко време в началото, но след това може да става абсолютно автоматично и да спести много главоболия, включително и при смяна на устройствата. Когато си купиш нов телефон или лаптоп, лесно може да прехвърлиш информацията от стария на новия.

3. Пази се от онлайн вируси

В онлайн пространството е от голямо значение да се предпазваме от вируси, които могат да ни навредят. Ето няколко ключови подхода за това:

- Използвай най-актуалната версия на добра и лицензирана антивирусна (и антималуер) програма.
- Обновявай си операционните системи, приложенията и програмите.
- Не отваряй съмнителни линкове, реклами и имейли от непознати.
- Избягвай несигурни мрежи (отворен Wi-Fi).
- Внимавай при използването на USB флаш памет.
- И не на последно място –използвай **firewall**.

4. Информирай се за актуалните измами в интернет пространството, за да не станеш жертва на такава

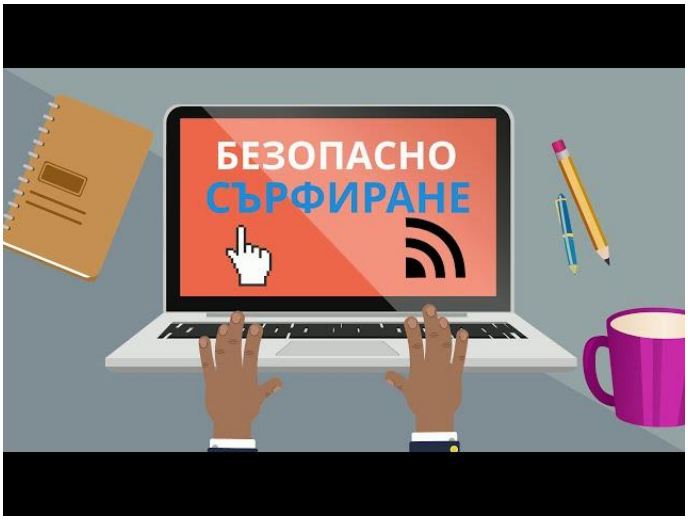
Понякога по новините или в социалните мрежи споделят за нашумяла измама – препоръчваме ти да не ги игнорираш. Важно е да се информираш, защото измамниците могат да бъдат много изобретателни в лъжите си. Ако предварително знаеш за този тип измама и попаднеш на нея, ще я разпознаеш и избегнеш лесно.

5. Не отваряй съмнителни имейли

Препоръчително е директно да изтриваш съмнителните (т.нар. фишинг) имейли, но ако все пак не си сигурен и ги отвориш – не следвай инструкциите им. Можеш да ги разпознаеш по следните признаци:

- Липсва поименно обръщение, а имейл адресът на подателя няма общо с името на институцията, от която уж е изпратен имейлът.
- В имейла те карат спешно да обновиш профила си или да изпратиш лична информация.
- Имейлът е написан с печатни или правописни грешки.
- Изискват от теб да последваш линк и да посетиш уеб страница или има прикачен файл, а подателят на имейла е неясен или съмнителен.

6. Внимавай в кои сайтове влизаш



Освен фишинг имейли, съществуват и фишинг сайтове. Принципът им на работа е същият, като гореспоменатия - представят се от името на съществуваща институция като обикновено е копиран и дизайнът на оригиналния сайт. Можем да ги разпознаем по уеб адреса - той също може много да прилича на истинския, но ще има някои разлики.

Друг сигнал е, ако връзката не е сигурна *(адресът не започва с https)*, трябва да си с повишено внимание. За тази цел препоръчваме да инсталираш приставката **WOT (Web of Trust)** към браузъра на компютъра си. Тя маркира нивото на безопасност на всеки сайт, който се появява.

Когато теглиш файлове, софтуер, игри или друго, също трябва да проверяваш сайтовете, от които смяташ да го направиш - като потърсиш мнения по независими форуми за тези сайтове.

7. Използвай само достоверни източници

Много е важно да можеш да разпознаеш истинските от лъжливите новини, особено по време на ситуация като пандемията с коронавирус. В социалните мрежи ежеминутно се споделят новини от цял свят във връзка с актуалната тема за COVID-19, но каква част от тях са истина и целят да информират хората за случващото се, а не да всяват паника или да получават някаква изгода от това?

Има неща, по които можеш да разпознаеш дали една новина е фалшива:

- Тиражирана е от съмнителна медия и не може да се намери в авторитетните издания.
- Написана е неясно и некачествено (напр. с печатни и правописни грешки).
- Няма снимки, които да докажат написаното, или кадрите са общи и неясни.
- Позовава се на неконкретни авторитети (напр. „британски учени“).
- Написаното в интернет и комуникираното по телевизията не винаги е вярно. Хубаво е да проверяваш информацията, особено ако ще я разпространяваш.

8. Внимавай какви приложения си качваш и какъв достъп им даваш

При регистрация внимавай какви данни попълваш и обръщай внимание на политиката за поверителност. Не споделяй лична информация публично (ЕГН, три имена, дата на раждане, адрес, телефонен номер и т.н.). Много често хората не четат политиката за поверителност и после остават изненадани от информацията, която може да се намери за тях в интернет.

9. Внимавай какъв дигитален отпечатък оставяш

Пробвай да се потърсиш в google и виж какво ще ти излезе. Трябва да знаеш, че сайтовете обикновено предоставят настройки за управление на данните ти, от които можеш да се възползваш.

10. Внимавай с кого и как общуваш

За съжаление онлайн не всеки е този, за когото се представя. Както в ежедневието, така и в интернет – не трябва да общуваш с непознати за теб хора. Тяхната цел може да не е в твой интерес.