Основни съвети за защита на личните ти данни онлайн (текст на информационно-разяснителна брошура, предназначена за деца)

Знаеш ли, че когато си в интернет и използваш социални мрежи (Instagram, Facebook, TikTok и др.) оставяш отпечатъци? Спокойно! Не става въпрос за следите от пръстите ти по мобилното устройство, а за дигитални следи!

Когато си онлайн, оставяш дигитална следа, която записва всичко, което правиш в различните сайтове и приложения, но и личните ти данни, които споделяш.

Ако изпълниш няколко лесни стъпки ще се защитиш по-добре:

1. Провери настройките на профила си в социалните мрежи

Когато си създаваш профили в социалните мрежи и отбележиш, че си под 18 г., е препоръчително да настроиш профилите си на поверителен режим. Ако профилът ти е в публичен режим или го промениш на такъв, тогава всеки може да види какво споделяш и коментираш, както и да ти изпраща съобщения. Винаги обмисляй много внимателно преди да изключиш настройките за поверителност, които са предназначени да те защитават.

2. Помисли преди да публикуваш

Независимо дали профилите ти са публични или поверителни, не забравяй, че след като публикуваш нещо онлайн, може да бъде трудно да го изтриеш. Така че преди да публикуваш нещо, запитай се дали наистина искаш то да е видимо за всеки, години наред в интернет.

3. Отнасяй се с данните на другите така, както се отнасяш със собствените си данни

Послушай близките си преди да публикуваш нещо или когато те помолят да изтриеш снимки или видеоклипове с тях! Един ден може да поискаш и те да направят същото за теб.

4. Внимавай, когато се отбелязваш (тагваш)

Помисли и преброй до 10 преди да се отбележиш от някое място, защото като споделяш местоположението си, можеш да се изложиш на риск. Не давай разрешение на приложението или сайта да използва местоположението ти, освен ако не ти е необходимо.

5. Не се оставяй да бъдеш „подведен"

Понякога сайтовете и приложенията се опитват да те подведат, като искат да предоставиш повече лична информация, отколкото им е необходима. Обичайно бутонът, върху който искат да кликнеш, е голям, ярък и в средата на екрана, докато другата опция е малка и се пропуска лесно. Внимавай за тези практики и избери опцията, която е най-сигурна, а не най-лесната за кликване!

6. Без да бързаш, внимателно прочети условията

Всеки сайт или приложение трябва да ти предостави информация за това какво прави с личните ти данни. Често тази информация е написана на сложен и неразбираем език, затова ако не си сигурен, попитай родител или потърси човек, който да ти даде компетентен съвет.

7. Не кликвай просто върху „Приемам всички" (Accept all)

Видиш ли съобщение за поверителност или банер за бисквитки, помисли дали искаш да ги приемеш. Потърси бутона, който ти позволява да отхвърлиш тези, които можеш. В противен случай споделяш повече лична информация, което може да ти навреди.

8. Знай стойността на личните си данни

„Безплатните" услуги не винаги са безплатни. Голяма част от личните данни, споделяни онлайн се използват от приложенията и сайтовете, за да се печелят пари от неща като реклами. Винаги се питай дали си заслужава да споделяш твоите лични данни и получаваш ли справедлива сделка срещу тях.

9. Не забравяй, че контролът е в теб

Когато споделяш личните си данни, ти имаш права върху тях, за които сайтовете и приложенията трябва да се съобразяват. Например ти можеш да поискаш от тях достъп и копие от личните ти данни или да изтрият профилите ти.

10. Дръж родителите си в течение

Никога не лъжи за възрастта си, когато се регистрираш в социалните мрежи! Това може да е опасно за теб. Дори да си сигурен, че контролираш личните си данни, винаги е добра идея родителите ти или възрастен, на когото имаш доверие, да имат информация за действията ти и най-вече при необходимост от помощ, да се обърнеш към тях.

11. Изтрий профила си, когато нямаш нужда от него

Ако вече не използваш някое приложение или сайт, по-добре изтрий профила си, защото той може да бъде хакнат след време и да се използва от други хора, а това може да ти навреди.

12. Създавай си силни пароли

За да запазиш личните ти данни, си измисли силни пароли. Силна парола е тази, която съдържа поне 12 знака, от които има малки и големи букви, цифри и специални символи. Старай се да е колкото може по-необичайна и оригинална. Не използвай пароли, които са свързани с очевидни неща, които някой друг може да познае, като например името на домашния ти любимец или любимото ти телевизионно или интернет предаване. Ако можеш използвай мениджър за пароли.

Пример за силна парола: wH-1289757_etV#

13. Не използвай една и съща парола за всичко

Когато използваш една и съща парола за всеки от профилите си, излагаш личните си данни на риск. Затова никога не използвай една и съща парола два пъти. Ако някой разбере твоята парола, която използваш на много места, то ти ще бъдеш уязвим.

14. Ако нещо ти изглежда подозрително, не кликвай върху него

Получавал ли си съмнително съобщение от непознат или дори от приятел? Това може да е някаква измама. Не го отваряй, не кликвай върху никакви линкове и го изтрий веднага, колкото и да си любопитен. По-добре в безопасност, отколкото да съжаляваш.

15. Използвай само защитени Wi-Fi мрежи

Може да ти изглежда лесно, когато просто кликваш и се присъединяваш, но незащитените мрежи са много рискови. Хакер, използващ същата мрежа, може да открадне данните ти или дори да поеме контрола върху твоето устройство.

16. Поддържай устройствата си актуални

Винаги е изкушаващо да кликнеш върху бутона „Напомни ми по-късно” (remind me later), когато устройството ти поиска да инсталираш актуализация. Трябва да знаеш, че тези актуализации често съдържат важни защити срещу най-новите вируси и измами. Винаги инсталирай актуализациите възможно най-скоро.

Как да се свържеш с нас?

Ако имаш въпроси за защитата на личните си данни, можеш да потърсиш информация на нашия уебсайт: https://www.cpdp.bg/

Настоящият информационно-разяснителен материал е изготвен съвместно от Комисията за защита на личните данни и Съвета на децата към председателя на Държавната агенция за закрила на детето.