Yettel.

Какво не трябва да се споделя в интернет

Знаете ли, че когато сме в интернет и използваме социални медии, оставяме отпечатъци? Разбира се, не става въпрос за следите от пръстите ни по мобилните ни устройства, а за дигитални следи. Всички ние – възрастни и деца, оставяме дигитални следи, които записват всичко, което правим в различните сайтове и приложения, но и личните данни, които споделяме. Когато става дума за децата в интернет, защитата на личните данни е от първостепенна важност. Използването на социални мрежи и други онлайн платформи може да бъде забавно и образователно за децата, но също така и със сигурност рисковано, ако не направим профилите на децата сигурни и не ограничим видимостта на личната информация, която приложенията ни изискват при регистрация.

Като например съобразяването на профилите им в социалните медии спрямо възрастта, проверяването на поверителността на сайтовете, в които се регистрират и като цяло – ограничаването на видимостта на личната информация, която приложенията изискват при регистрация.

Много е важно преди децата да са в мрежата и социалните медии да ги научим какво са лични данни и как може да се злоупотреби с тях, и да развиваме у децата умения за изграждане на „защитни стени“ в интернет. Важно е да развиваме и критичното им мислене, за да сме сигурни, че могат да взимат информирани решения за тяхната онлайн активност.

С какво да започнете?

1. **Обяснете на детето какво са лични данни.** Лични данни са трите ни имена, рождена дата, телефонен номер и имейл (защото са свързан с името ни), адрес и данните като ЕГН, номер на лична карта и шофьорска книжка. Ако имат достъп до тях, престъпниците в мрежата могат лесно да ги използват за злоупотреби – могат да създават фалшив профил с вашето име, да извършват финансови измами и др.
2. **Насърчавайте го да уважава личните данни на другите.** Обяснете на детето защо не трябва да споделя лична информация, снимка и дори локация за своите приятели или семейство без тяхното съгласие. Подтиквайте го да бъде толерантно в интернет и да не разпространява информация за връстниците си.
3. **Активирайте настройки за безопасност.** Проверете дали профилите на детето са настроени в поверителен/частен (private) режим, особено ако детето е под 18 години. Публичните профили излагат децата на значително количество и различно по вид вредно съдържание, прави ги видими и достъпни за много хора в мрежата, включително нежелани контакти и ги излага на коментари, които не винаги са добронамерени. Не забравяйте да активирате двуфакторната верификация, която защитава допълнително профилите му от хакване.
4. **Създайте му рефлекс „Мисли, преди да публикуваш“.** Обсъдете с детето важността да помисли внимателно, преди да споделя нещо онлайн. Разгледайте заедно няколко негови публикации и го попитайте „Какво искаш да кажеш с тази снимка?“, „Какво е посланието на последното ти видео?“, „Какъв е изводът в последната ти публикация, какво могат хората да научат за теб от това, което

качваш в мрежата?“. Дискутирайте какво би искало приятелите му и непознати хора онлайн да научават за него и дали публикуваната информацция го прави уязвимо. Нека разбере, че веднъж публикувани, информацията, снимката, видеото, започват да водят свой собствен живот и дори да бъдат изтрити от профила на детето ви, те може да продължат да циркулират из мрежата. Ако има хора, които са свалили съдържанието или са направили скриншот, то може да бъде видимо в интернет години наред.

5. **Научете детето да бъде внимателно с отбелязването на местоположението си.** Запознайте го с рисковете, които произлизат от споделянето на точната му локация, и поговорете с него дали е необходимо да се „отбелязва“ в социалните медии. Покажете му как да изключи автоматичното разрешаване на приложението или сайта да използва/отбелязва местоположението му. Регулярно му напомняйте да бъде внимателно, когато се тагва със свои приятели и че е важно да го прави само ако те са съгласни.
6. **Предупредете го за съмнителните съобщения и линкове.** Поговорете с детето за фишинга, който все повече се среща в социалните мрежи, и каква е неговата цел. Покажете му как да разпознава дали съобщенията са истински или фалшиви – като преглежда внимателно подателя, следи за лош правопис и съмнителни искания в имейла. В началото е добре да се съветва с вас преди да кликва на дадени линкове. Дайте му примери с потърпевши деца и възрастни, които са загубили профилите си, защото са реагирали на фалшиво съобщение за нарушаване на правилата на дадена социална мрежа. Връщането на профил е много трудна задача, а децата държат на тях, особено в тийнейджърска възраст.

Като родители имаме възможността да помагаме на децата да бъдат информирани и да правят осъзнати решения за своя виртуален живот. С проактивност, споделяне на опит и внимание можем да ги научим да бъдат отговорни и защитени дигитални граждани.

Съвети към родителите:

- **Проверявайте условията** за ползване и данните, които събират сайтовете и приложенията, използвани най-често от детето ви. Преразкажете му го на достъпен и разбираем език. Помогнете му да разбере, че трябва да бъде внимателно с данните, които споделя.
- **Научете детето да създава силни и различни пароли** за приложенията си и се уверете, че ги използва. Можете заедно да проверите колко са силни паролите му на https://www.security.org/how-secure-is-my-password/. Обърнете му специално внимание, че за по-голяма сигурност, паролите трябва да се променят на всеки 6 месеца, дори само с един знак.
- **Поддържайте отворена комуникация** с детето относно неговите онлайн дейности. Инициирайте разговорите не чрез контрол – те винаги го усещат и се затварят, а като проявявате загриженост и интерес към неговия виртуален свят. Уверете го, че може да говори с вас винаги, ако се почувства неудобно или ако се сблъска с нещо съмнително онлайн и офлайн.
- **Бъдете пример за подражание** – подрастващите правят това, което виждат у родителите си. Споделяйте с детето какво сте видели в интернет, изпращайте му интересни и поучителни клипчета, споделяйте му, когато сте обновили паролата

си или ако сте видели лични данни в профила на ваш познат. Така неусетно ще му показвате как да бъде отговорно и разумно в интернет.