ПРАВИЛА ЗА БЕЗОПАСЕН ИНТЕРНЕТ

1. Пазете личната си информация

Не е нужно всички да знаят кои са Ви приятелите или какъв е домашният Ви адрес. Можете сами да избирате с кого какво да споделяте. Не бихте предоставили току така личната си информация на непознат, не я споделяйте с милиардите потребители онлайн.

2. Използвайте настройките за безопасност

Хората, които се занимават с реклама, и хакерите биха искали да знаят повече за Вас. И едните, и другите могат да научат много от Вашия бразуър и от социалните мрежи. Социалните мрежи, мобилните приложения и браузърите имат настройки за защита на личните данни. Намерете ги и ги настройте по Ваш избор.

3. Използвайте функцията за безопасно сърфиране

Не бихте се разхождали в опасен квартал, не посещавайте и опасни сайтове в интернет. Киберпрестъпниците използват по-сензационно съдържание или фалшиви реклами като примамка. Дигиталният свят е изпълнен с трудно забележими капани и едно невнимателно кликване може да даде достъп до личните Ви данни или да зарази устройството Ви със злонамерен софтуер.

4. Проверявайте дали интернет връзката Ви е безопасна

Когато влизате в интернет на публично място, например през незащитена с парола публична WiFi връзка, се поставяте под риск. Ако имате възможност, изчакайте по-подходящ момент да се свържете, когато имате сигурна WiFi връзка.

5. Внимавайте какво сваляте от Мрежата

Основна цел на киберпрестъпниците е да Ви подведат да си свалите зловреден софтуер или да достигнат до личните Ви данни. Зловредният софтуер може да бъде замаскиран като всякакво приложение, програма или игра. Не сваляйте приложения, които изглеждат подозрителни или се намират на сайт, на който не можете да се доверите.

6. Използвайте силни пароли

Използвайте трудни (дълги, с главни и малки букви, цифри и специални знаци) и различни за всеки сайт пароли. Можете да ползвате и програма за управление на паролите, за да не се налага да ги запомняте всичките.

7. Внимавайте какво публикувате

Всяка публикация или коментар онлайн остава в Мрежата завинаги. Понеже и да изтриете поста си (напр. във Фейсбук), това не изтрива и копията (напр. екранни снимки/ скрийншотове), които може други вече да са си направили. Не пишете и не качвайте нищо, което може да ви дискредитира.

8. Внимавайте с кого общувате онлайн

Хората, с които се запознавате онлайн, не винаги са тези, за които се представят. Фалшивите профили в социалните мрежи са предпочитан от хакери, измамници и педофили начин да Ви подведат. Опитайте се да проверите дали човекът отсреща наистина е този, за когото се представя чрез проверка по име, имейл, снимка и контролен въпрос, на който би трябвало да знае отговора, ако е наистина този. При съмнение можете да подадете сигнал или да потърсите съвет през сайта на Центъра за безопасен интернет www.safenet.bg.

9. Използвайте актуализирана антивирусна програма

Използвайте антивирусна програма и редовно я обновявайте. Поддържайте и последните актуализирани версии на всички програми и приложения.

10. Предпазвай се и реагирай в случай на онлайн тормоз

Ако някой Ви обижда или тормози онлайн, не отговаряйте. Докладвайте го на самия сайт или на Центъра за безопасен интернет и го блокирайте. Направете екранна снимка (скрийншот) на съответния разговор или съдържание като електронно доказателство.