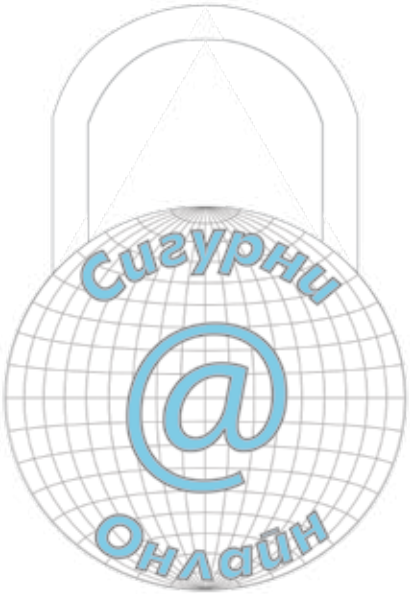
Co-funded by
the European Union

Multi Ethno Forum

СИГУРНИ ОНЛАЙН

РЪКОВОДСТВО ЗА БЕЗОПАСЕН ИНТЕРНЕТ



Проект "Сигурни Онлайн"
с номер 2023-1-BG01-KA154-YOU-000141767
е съфинансиран от програма Еразъм+ на ЕС.

Какво трябва да знаем когато сме в Интернет?

Интернет (наричан още "Глобалната мрежа") може да е много приятно и интересно място за прекарване на свободното време. В него спокойно може да намерите изобилие от информация, интересни факти, забавни клипчета и игри. Ако знаете как да я ползвате, Глобалната мрежа е може би най-полезното изобретение на нашето време. Възможностите й са необятни.

Но Интернет крие и своята тъмна страна. Тъй като е създаден от хора като място за свободно споделяне на информация, знания и всичко, което ни интересува, в него съществуват същите опасности, каквито са в реалния свят - навън на улицата. Да, в Интернет не може да Ви блъсне автомобил, но могат да Ви се случат също толкова неприятни и опасни неща.

Тук ще Ви покажем какво ни заплашва и как да се пазим в Глобалната мрежа. Ако отново дадем пример с улицата: Ще научите за какво да се оглеждате в Интернет и как правилно да пресичате в мрежата.

Кои са опасностите:

Злонамерен софтуер - Вируси

Злонамереният софтуер се дегизира като надежден (познат за вашето устройство) прикачен файл към имейл, чат или програма (т.е. може да е препратка към друг сайт, снимка, клипче, игра или друга програма). Вирусите може да "работят" самостоятелно или да дават достъп на други хора (хакери) до вашето устройство и цялата информация в него. Този тип кибератака често прекъсва работата на цялата ИТ мрежа. Някои примери за злонамерен софтуер са троянски коне, шпиониращ софтуер, червеи, вируси и рекламен софтуер.

Фишинг

Фишинг е изпращането на измамнически имейли и съобщения от името на реномирани фирми. Хакерите използват фишинг, за да получат достъп до личните ви данни, банкови сметки, контакти и други

Фалшиви Новини

Фалшивите новини са публикации, които имат за цел да ви измамят. В най-честия случай иде реч за финансова изгода или политическа пропаганда. Те най-често се разпространяват в социалните мрежи като Facebook, X, Instagram, TikTok и др., защото няма цензура или редактори, които да проверяват информацията.

Как да разпознаем фалшивата новина:

- Вижте източника
- Проучете автора
- Проверете датата
- Прочетете целия текст, а не само заглавието
- Вижте дали има посочени източници на информацията
- Проверете дали новината съществува в реномирани и проверени сайтове.

Какво представлява кибертормозът?

Кибертормозът е тормоз чрез дигиталните технологии. Може да се случи в социалните мрежи, платформите за съобщения, платформите за игри и през мобилните телефони. Това е повтарящо се поведение, целящо сплашване, ядосване или засрамване на потърпевшите.

Кибертормозът включва:

Разпространяване на лъжи или публикуване на неприлични снимки на някого в социалните мрежи; Изпращане на обидни съобщения или заплахи през платформите за съобщения; Изпращане на злонамерени съобщения под чужда самоличност на други хора.

Тормозът лице в лице и кибертормозът често се случват паралелно. Но кибертормозът оставя електронна следа – която е много полезна и служи като доказателство пред полицията и съда за прекратяване на подобно поведение.

Защита

Въпреки че приложенията и устройствата за защита, като например антивирусни програми и защитни стени срещу злонамерен софтуер, са от съществено значение, но не е достатъчно просто да включите тези инструменти и да мислите, че всичко е наред.

За по-надеждна защита - следвайте тези стъпки:

Архивни копия на данни

Важните за вас данни трябва да се съхраняват в защитено място, външен твърд диск или флаш памет, ползвайте защитени облачни пространства.

Добри кибер навици

Не отваряйте неочаквани връзки или прикачени файлове, които може да получите в имейл или текст, дори ако изглежда, че идват от надежден подател.

Използвайте силни, уникални пароли

Добрите пароли трябва да са дълги най-малко 14 знака, не трябва да са английски думи и не трябва да се използват повторно в няколко акаунта, трябва да съдържат големи и малки букви, цифри и специални знаци като: @ # $ %. Сменяйте паролите често и задължително при съмнение за нередност.

Поддържайте софтуера си актуализиран

Всички операционни системи като Windows, MacOS, iOS или Android, както и приложенията и браузърите трябва да се актуализират с най-новите обновявания, особено на сигурността от производителя.

Нека обобщим

- Не вярвайте на случайни имейли, обаждания и съобщения
- Ползвайте защитени мрежи
- Подберете и сменяйте често паролите си
- Не забравяйте да актуализирате телефона и компютъра си
- Не споделяйте лична информация в интернет
- Не отговаряйте на непознати
- Не влизайте в пиратски сайтове
- Инсталирайте програми и игри само от проверени източници
- Не споделяйте интимни снимки дори на шега
- Не се снимайте голи или по бельо
- Не използвайте чужди устройства, за да влизате в своите акаунти

Ако сте обект на кибертормоз, съмнявате се, че сте жертва на кибератака или не сте сигурни дали това което четете и виждате е истина – попитайте родител, учител или по-възрастен ваш близък, на когото имате доверие.

Ако вие сте в подобно положение или познавате дете в такава ситуация и се страхувате, срамувате и не знаете какво да правите може да се свържете с:

ОТДЕЛ ЗА ЗАЩИТА НА ДЕТЕТО,
Да се обадите в ПОЛИЦИЯТА,
звънете на тел: 116111 за деца жертви на насилие
или да посетите https://www.sapibg.org/bg

Co-funded by the European Union

Сигурни @ Онлайн

Multi Ethno Forum

Проект "Сигурни Онлайн"с номер 2023-1-BG01-KA154-YOU-000141767
е съфинансиран от програма Еразъм+ на ЕС. Публикацията излага единствено възгледите на автора, като програмата и Европейската комисията не носят отговорност за изчерпателността и верността на информацията, посочена тук, нито за възможните начини за нейната употреба.