

Поверителност в социалните медии:

Контрол на личната информация - Контролът на личната информация се отнася до способността на лицата да управляват и да имат правомощия върху собствените си лични данни. Това включва правото да решават каква информация да се събира за тях, как да се използва и с кого да се споделя. В контекста на неприкосновеността на личния живот и защитата на данните, контролът на личната информация подчертава значението на индивидите, които имат автономията да правят информиран избор относно събирането, обработването и разпространението на техните лични данни.

Осъзнаване на настройките за поверителност - Настройките за поверителност се отнасят до конфигурируемите опции в дигиталните платформи, приложения или устройства, които позволяват на потребителите да контролират и управляват видимостта, достъпността и споделянето на тяхната лична информация. Тези настройки дават възможност на хората да персонализират своите предпочитания за поверителност, като определят кой има достъп до техните данни, преглежда съдържанието им или взаимодействия с тях онлайн.

Сигурност на данните, включително снимки - сигурността на данните включва защита на дигитална информация, включително снимки, от неоторизиран достъп, разкриване, промяна или унищожаване. Това включва мерки и протоколи, предназначени да защитават чувствителни данни, като гарантират тяхната поверителност, цялост и наличност, особено в дигитални среди.

Обмислено публикуване и споделяне - внимателно обмисляне и целенасочено споделяне на съдържание, като мисли, мнения или медия, с осъзнаване на потенциалното му въздействие върху себе си и другите. Този практика набляга на отговорността, съпричастността и внимателния подход към онлайн комуникацията.

Съгласие и маркиране - получаване на разрешение преди включване на някого в публикация, снимка или онлайн съдържание и изричното им идентифициране с помощта на тагове. Тази практика зачита

поверителността на хората и им позволява да контролират своето онлайн представяне.

Като цяло е важно младежите и възрастните хора да бъдат проактивни в защитата на поверителността си в дигиталната среда. Като сме информирани, използваме сигурни практики и внимаваме за нашите онлайн дейности, можем да минимизираме потенциалните рискове и да постигнем по-безопасно онлайн изживяване.

Какво означава онлайн безопасността ?

Онлайн поверителността и прилагането на набор от инициативи за безопасност по отношение на защитата на личните данни и личната информация означава:

- ✓ Да познавате и прилагате основни правила и принципи за безопасност, защита на неприкосновеността на личния живот и личната информация;
- ✓ Да прилагате настройки за поверителност и разрешения като бисквитки, да сте запознати с инструментите за проследяване, да сте наясно с вашия дигитален отпечатък;
- ✓ Да бъдете осведомени относно стратегиите и инструментите, използвани в момента за проследяване, шпиониране и навлизане в личната сфера.
- ✓ **Сигурните методи за онлайн плащане** се отнасят до електронни транзакции, извършвани чрез интернет, които дават приоритет на защитата на чувствителна финансова информация, като гарантират поверителността, целостта и автентичността на процеса на плащане. Тези методи използват усъвършенствани технологии за криптиране и протоколи за сигурност за защита на финансовите данни на потребителите, предотвратявайки неоторизиран достъп и измамни дейности. Основните характеристики на сигурните онлайн методи за плащане включват:
 - ✓
 - ✓ **Шифроване:** Използването на алгоритми за криптиране за кодиране на финансова информация по време на предаване, което я прави нечетима за неоторизирани страни. Secure Sockets Layer (SSL) и Transport Layer Security (TLS) са общи протоколи за криптиране.

✓

- ✓ **Токенизация:** Замяната на чувствителни данни с уникален идентификатор или токен. Това помага за защитата на действителните финансови подробности, тъй като дори и да бъде прихванат, токенът няма значима информация.

✓

- ✓ **Двуфакторно удостоверяване (2FA):** Допълнителен слой на сигурност, изискващ от потребителите да предоставят две форми на идентификация, преди да извършат транзакция. Това често включва парола и временен код, изпратен до мобилното устройство на потребителя.

✓

- ✓ **Шлюзове за защитени плащания:** Шлюзовете за плащане действат като посредници между уебсайта на търговеца и финансовата институция, като сигурно обработват транзакциите. Уважаваните и сигурни шлюзове за плащане се придържат към индустриалните стандарти за защита на данните.

✓

- ✓ **Откриване и предотвратяване на измами:** Внедряване на инструменти и алгоритми за откриване и предотвратяване на измамни дейности, като необичайни модели на покупка или множество неуспешни опити за влизане.