

# МИТ ХАКЕРИТЕ НАБЕЛЯЗВАТ САМО ПЛАТЕЖОСПОСОБНИ ЖЕРТВИ

## Всеки може да стане жертва на хакерска атака.

Хакерите се стремят към най-голямата награда, постигната с минимални усилия, което най-често води до набелязване на бази данни с информация за много хора. Ако за теб има информация в подобна база данни, то тя може да попадне в ръцете на хакери и да бъде използвана за злонамерени цели. Важно е да бъдеш внимателен, когато предоставяш информация в мрежата, да се запознаеш с „Правила и условия на ползване“ при регистрирането на лична информация в сайтове, както и да проучиш предварително съответната компания.

### Минимизирай риска:

**Контактувай** с компании, които познаваш – преди да предоставиш лична или финансова информация, се увери, че това е компания с репутация. Хакерите често създават сайтове, които изглеждат легитимни.

**Не подценявай** качеството на паролите си – дават ниво на сигурност, ако бъдат използвани прилежно.

Отдели време **да се запознаеш** с политиките за сигурност – запознай се как компанията ще използва/съхранява твоята лична информация.



### Минимизирай риска:

- Бъди внимателен каква информация споделяш в мрежата – Хакерите могат да обединяват информация от различни източници, избягвай публикуването на лична информация в обществени форуми.





Паролата ти за WiFi трябва да бъде достатъчно надеждна:

**X** Без рождени дати и имена

**X** Никога „123456“

Ако има свързано устройство, което не разпознаваш, веднага смени паролата/името на WiFi мрежата.

**ВИНАГИ** Периодично сменяй паролите си –не използвай една и съща парола за множество потребителски имена.

**ВИНАГИ** Изключвай рутера си, ако не го използваш.

**ВИНАГИ** Криптирай:

-чувствителните файлове на компютъра си;

-съдържанието на мейлите си при изпращане.

**ВИНАГИ** Сменяй административните пароли, които са предварително зададени на устройствата.

*Не използвай публично достъпни WiFi мрежи, ако имаш чувствителна информация на устройството си. Рисуваеш пробив на устройството и кражба на информацията.*

