

#### Rizika:

1. Odcizení osobních souborů(třeba nám můžou ukrást nějaký super SW)
2. Umožnění přístupu do uzavřené sítě(můžou pak ukrást data organizace)
3. Ukradení bankovních informací(můžou nám vyluxovat konto)
4. Pokud nám někdo ukradne soc. síť může za nás postovat(budou dávat pro ruské posty atd.)
5. Může nás někdo sledovat přes kameru nebo odposlouchávat přes mikrofon(No comment)
6. Může využít HW pro těžbu Bitcoinu(Hodně to zpomaluje počítač ale hlavně z toho nemáme ani korunu a někdo na náš účet bohatne)
7. Možnost sledování polohy(stalkování z postele)
8. Naletet na internetový podvod(přijdeme o hodně peněz)
9. Přihlašovat se na veřejné nezaheslované wifi(může nás odposlechnout)
10. Stát se závislým (:DDD)

#### Řešení:

1. Mít silné hesla
2. Při brousdání na deep webu využívat VPN
3. Nestahovat z pochybných stránek
4. Využívat virtuální počítač
5. Používat vlastní internet (mobilní data => hotspot)

#### Zamyšlení:

1. Heslo: mít silné hesla která se nepakují
2. Mazání souborů: bez nějakých pomocných souborů nelze ve win10 úplně odstranit data aniž bychom je přepsali
3. Sociální síť: velký problém lidé na ně zveřejňují kompletně svůj život
4. Likvidace starého počítače: Ani dáním pc do továrního nastavení se vše nevymaže pokud byto byl problém je nutné disky prodat jinak
5. Převoz výpočetní techniky: Pokud je nutné zabezpečit informace převážet disk a pc zvažt jinak stačí ochrnná brašna která sníží otřesy mechanických částí
6. Údržba počítače: Dobré mít zapnutou defragmentaci disku, lepší mít antivirus pro lepší ochranu počítače
7. Autorský zákon: Správné citování.