Bezpečný internet

Život bez prístupu na internet si v dnešnej dobe vieme predstaviť veľmi ťažko. Počítače, tablety, smartfóny, digitálne hodinky, či herné konzoly. To je ešte úzky výber technologických výdobytkov, ktoré nás neustále obklopujú a my ich využívame na dennej báze.

Európska komisia prostredníctvom Programu pre bezpečnejší internet podporuje Deň pre bezpečnejší internet. Jeho organizáciu na celom svete zabezpečuje sieť INSAFE od roku 2004. Hlavným cieľom je zvýšiť informovanosť o bezpečnejšom a lepšom internete, kde má každý možnosť používať technológie zodpovedne, s úctou, kriticky a tvorivo. Zmyslom je upozornenie na ochranu súkromných údajov na internete, najmä na webových stránkach sociálnych sietí.

Mnohé spoločnosti podpísali Zásady pre bezpečnejšie sociálne siete a umožnili tak užívateľom ľahšie meniť nastavenia ochrany súkromia. Každý z nás, bez ohľadu na vek, by mal byť opatrný a vyvarovať sa rizikám súvisiacim s používaním internetu, tak aby mohol v čo najväčšom rozsahu využívať mnohé z užitočných výhod, ktoré internet v dnešnej dobe ponúka. O tom, aké nebezpečenstvá môžu hroziť pri využívaní internetu, dostávajú informácie nielen žiaci v školách, ale aj ich rodičia.

Bezpečný internet bez nenávistných prejavov, kyberšikany, phishingu (typ počítačového útoku, pri ktorom sa podvodník snaží v komunikácii získať od používateľov osobné údaje) či explicitného obsahu je dávno minulosťou. Aj z týchto dôvodov si pripomíname Deň pre bezpečnejší internet, ktorý tento rok pripadá na pondelok - 8.február.

Otázka znie ako sa chrániť v dobe digitálu, kedy už bežné surfovanie internetom nie je považované za bezpečné? Odpovedí na túto otázku je niekoľko od množstva odborníkov.

Na zhrnutie možno uviesť 11 tipov na to ako pri surfovaní po internete na svojom smartfóne, tablete či počítači zostať v bezpečí:

1. Na sociálnych sieťach rozmýšľajte dvakrát a zdieľajte obsah s rozumom.
2. Dajte si pozor na online hry zadarmo, ktoré môžu obsahovať malvér (zahŕňa všetky druhy škodlivého softvéru vrátane najznámejších foriem, ako sú trójske kone, ransomware, vírusy, červy a bankový malvér) a pár chvíľok zábavnej hry vás môže stáť aj zneužitie vašich osobných údajov.
3. Pozor na otvorenú WiFi, ktorá môže byť napadnutá hekermi (počítačoví piráti, ktorý prenikajú do cudzích počítačov či databáz, aby získali prístupové práva) .
4. Dômyselne vyberajte vaše heslá a často ich meňte.
5. Kontrolujte si vaše nastavenia súkromia.
6. Dobre rozlišujte nevyžiadanú reklamu vo forme spamov (*hromadne rozosielaná správa* prakticky rovnakého obsahu) a phishingu, neotvárajte prílohy podozrivých emailov.
7. Používajte antivírusové programy a bránu firewall (prvý ochranný štít vašej siete).
8. Starostlivo si zálohujte vaše dáta.
9. Buďte pripravení na útoky hekerov a reagujte rýchlo.
10. Nezabúdajte sa odhlásiť z vášho konta.
11. Dajte prednosť https pred http (https webstránky sú zabezpečené, u http sa neodporúča poskytovať svoje osobné údaje).