certSIGN

Cyber4Kids

LECŢIA 7.
WiFi sau nu?

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – BAGHETA ÎNCREDERII! Ea te va ajuta să te conectezi în siguranţă la Internet şi vei şti ce reţele sunt în regulă pentru tine!

1 **PE INTERNET, PRIN WIFI.** Pentru a intra pe Internet, trebuie doar să te conectezi on-line de pe telefon, tabletă sau calculator. Una din uşile pe care poţi intra în Internet este reţeaua WiFi. O foloseşti acasă, la şcoală sau din locuri publice – muzee, parcuri, restaurante, magazine, aeroporturi sau hoteluri. Însă, dacă la reţeaua WiFi de acasă te conectezi doar tu şi familia ta, la celelalte oricine poate avea acces. Inclusiv răufăcătorii on-line!

2 **CUM TE PROTEJEZI?** Respectând de fiecare dată aceste sfaturi:

• **Ai grijă la ce WiFi te conectezi.** Chiar dacă include denumirea locului în care te afli, asta nu înseamnă că acea reţea nu a fost făcută de un răufăcător şi nu este o capcană!

• **WiFi-urile publice pot să nu fie sigure.** Chiar dacă există o cheie - o parolă - pentru a le accesa, şi un infractor o cunoaşte. Poate fi chiar persoana de la masa de lângă tine, dintr-un restaurant, care va putea să vadă ce mesaje trimiţi, să îţi descopere parolele sau să îţi acceseze conturile.

• **Nu introduce date personale în site-uri, conectat de pe WiFi-uri publice.** Nu ştii cine poate să le vadă atunci când stai pe Internet folosind o conexiune care nu este sigură! Alte persoane din aceeaşi reţea pot vedea ce trimiţi şi pot avea acces la informaţiile tale personale, contacte, poze, nume de utilizator şi parole.

• **Nu lăsa telefonul, tableta sau laptopul să se conecteze automat la WiFi.** Roagă-i pe părinţi să oprească această funcţie din dispozitivele tale.

• **Nu instala aplicaţii şi nu accesa site-uri şi linkuri necunoscute de pe WiFi-uri publice**. Asigură-te că linkurile pe care ai intrat au în faţa adresei un lacăt închis şi încep cu HTTPS.

PAGINA PĂRINȚILOR

1. WIFI PRIVAT, PUBLIC SAU CONEXIUNI MOBILE? Explică-i copilului principalele diferenţe dintre mijloacele de conectare la Internet: WiFi-ul privat, de acasă (plătit, securizat, care poate fi accesat doar de către voi prin introducerea unei parole secrete - nu şi de către vecini), WiFi-ul din locuri publice precum muzee, parcuri, restaurante, magazine, aeroporturi sau hoteluri (deschis pentru oricine care cunoaşte parola, atunci când aceasta există, şi nu la fel de sigur) şi datele mobile (conexiune pentru telefoane, tablete, plătită şi limitată, care poate genera costuri suplimentare).

2. RISCURILE REŢELELOR PUBLICE DE WIFI. Pentru ca cel mic să înţeleagă de la tine de ce nu este indicat să folosească reţele WiFi cu acces liber, trebuie mai întâi să ştii tu care sunt riscurile acestora:

• **Man-in-the-Middle (MitM)**. Un atac MitM presupune interceptarea unei comunicări între două sisteme, de către o terţă parte externă. Indiferent despre ce vorbim (e-mail, rețele de socializare, navigare pe Internet), infractorii cibernetici pot intercepta direct comunicarea atunci când te conectezi la o reţea WiFi necriptată, riscând alterarea mesajelor, furtul datelor personale, a informaţiilor de pe dispozitiv (parole, informaţii bancare etc.).

• **Malware**. Atacatorii te pot păcăli să descarci conținut de tip malware atunci când te conectezi la un WiFi public. Pericolul programelor malware (viruşi, viermi informatici, spyware, adware, troiani) poate varia de la infectarea dispozitivelor, furtul de informaţii personale, vizualizarea fişierelor off-line precum fotografii și documente sensibile, până la accesarea camerei și microfonului, astfel încât altcineva să ştie ce faci şi în lumea reală, nu doar on-line.

• **Hotspot-uri maliţioase.** Infractorii cibernetici pot seta un hotspot într-o zonă publică, denumindu-l “WiFi Public” sau după o cafenea, un magazin ori sediul unei firme din apropiere. Aflându-te în căutarea unei conexiuni gratuite la Internet, un astfel de nume îţi poate părea legitim şi poţi deveni uşor victima atacatorilor care îţi vor spiona activitatea on-line, fără să îţi dai seama că eşti în pericol.

3. SSL ŞI VPN LA PUTERE! Mai ales pe WiFi-uri publice, trebuie utilizate conexiuni SSL (adică trebuie accesate doar acele site-uri care includ la începutul linkurilor un lacăt închis şi **HTTPS**). Acest protocol presupune criptarea traficului dintre dispozitivul tău și un site web, garantând autenticitatea celui din urmă şi făcând dificilă interceptarea comunicaţiilor de către intruși.

De asemenea, este indicat să foloseşti pe toate dispozitivele o soluţie **VPN** (Virtual Private Network) pentru securizarea activităţii pe Internet, criptarea traficului şi ascunderea adresei IP. Conexiunea sigură între tine și Internet creată de această rețea virtuală privată este esenţială pentru protejarea datelor personale în mediul on-line.