certSIGN

Cyber4Kids

LECŢIA 4.
Linkuri periculoase

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – BRĂŢARA REALITĂŢII! Ea te va ajuta să recunoşti linkurile false, în spatele cărora se ascund viruşi şi infractori cibernetici!

1. **VIRUŞI ŞI PROGRAME PERICULOASE.** Răufăcătorii de pe Internet îţi pot trimite linkuri în spatele cărora se ascund viruşi, programe şi mesaje periculoase, care îţi vor strica telefonul, tableta sau calculatorul ori îți vor fura datele personale, fără să îţi dai seama.

2. **CLICK AICI!** Ca să fie siguri că dai click, infractorii vor minţi şi vor spune că la acel link poţi vedea sau descărca un filmuleţ / un joc super amuzant. Sau îţi pot promite că, dacă intri pe acel site şi le dai date personale, vei câştiga mulţi bani, un telefon, o tabletă, o jucărie, noi puteri în jocul tău preferat on-line.

3. **CUM TE FEREŞTI?** Respectă de fiecare dată aceste sfaturi:
   - **nu da click pe orice link** de pe Internet sau pe care îl primeşti, mai ales dacă este de la o persoană necunoscută;
   - **nu crede** mesajele care îţi promit că vei primi ceva valoros – pe Internet nimic nu este gratis;
   - **nu descărca** jocuri, muzică, filme sau orice altceva din site-uri sau din e-mailuri trimise de persoane necunoscute;
   - **verifică** dacă linkurile pe care ai intrat au în faţa adresei un lacăt închis – acest lucru înseamnă că sunt sigure pentru tine;
   - **nu oferi date personale sau parole** în site-urile de pe Internet, în chestionare, ca răspuns la e-mailuri sau mesaje pe telefon;
   - **întreabă-i mai întâi pe părinţi** dacă ar fi bine să deschizi un link sau un site.

PAGINA PĂRINŢILOR

1. RISCURI. Explică-i copilului care sunt riscurile la care este expus – simpla accesare a unui link / site web sau descărcare a unui ataşament poate duce la instalarea automată de programe malware pe dispozitiv. Acestea pot oferi acces altor persoane la telefon, tabletă sau calculator.

2. PROBA PRACTICĂ. Învaţă-l cum să verifice autenticitatea link-urilor, site-urilor şi a e-mailurilor primite:

• **LINK.** Nu începe cu https:// ci cu http://? Lipseşte din faţa URL-ului (în partea stângă) un lacăt mic? **Nu este sigur.**

• **SITE.** URL-ul nu corespunde cu informaţia afişată în pagină (de exemplu, în adresa site-ului literele sunt înlocuite de cifre sau cuvintele sunt scrise greşit – c0npanle)? Lipseşte din pagină logo-ul? Sunt multe greşeli de scriere în textul afişat sau acesta este scris foarte mic? Apar multe pop-up-uri? Te anunţă că ai câştigat ceva? Solicită informaţii personale? **Nu este sigur.**

• **E-MAIL.** Nu recunoşti persoana / sursa care ţi-a transmis mesajul? Ţi se oferă ceva gratuit sau te anunţă că ai câştigat ceva? Mesajul ţi-a fost transmis on-line de un prieten dar când ai verificat cu acesta în realitate (obligatoriu) nu s-a verificat? Solicită informaţii personale sau parole? Sunt multe greşeli de scriere în textul afişat sau acesta este scris foarte mic? **Nu este sigur.**

3. SOLUŢII ANTIVIRUS. Curiozitatea este naturală pentru cei mici, ei fiind mereu atraşi de lucruri noi şi putând accesa cu ușurință linkuri maliţioase sau descărca jocuri din locații web necunoscute. De aceea, instalarea unei soluții antivirus, care include un motor de scanare în timp real, firewall și actualizare automată, este esenţială. O astfel de soluţie te ajută împotriva unor probleme precum spyware și viruși de pe site-urile pe care copilul le accesează.

Linkuri / site-uri aparent legitime pot conține coduri malware sau pot redirecționa către un site fals care arată la fel, dar care conține de fapt un keylogger (program care înregistrează fiecare bătaie de tastă şi salvează aceste date într-un fişier) sau un virus.

Efectuează periodic verificări automate de viruși şi scanări profunde ale sistemului, pentru a te asigura că nu există “vizitatori” nedoriţi şi că informațiile personale ale copilului nu sunt colectate.

4. SOLUŢII DE CONTROL PARENTAL. Cu ajutorul unei soluţii de control parental (atât pentru dispozitivele mobile, cât şi pentru cele desktop) puteţi monitoriza experiența pe Internet a copilului - de la timpul permis să-l petreacă on-line, până la aplicațiile și site-urile web utilizate / accesate. Încercările de utilizare a programelor blocate vor fi oprite și înregistrate în jurnalul programului, pentru vizualizare ulterioară.