NEWSLETTER nr. 2

Care sunt pericolele internetului pe care trebuie să le cunoști și de care trebuie să te ferești?

Pericolele de pe internet pe care trebuie să le cunoaștem, de care trebuie să ne ferim și cărora trebuie să le facem față atunci când este necesar pot fi rezumate în 9 mari categorii.

1) **Site-uri cu programe malware și viruși gata să vă infecteze calculatorul.**

Atunci când navigați pe internet, este foarte ușor să faceți clic pe un link greșit și să deschideți un site care încarcă programe malware pe computerul dumneavoastră. Din fericire, dacă aveți un antivirus actualizat instalat pe PC, acest virus va fi aproape întotdeauna oprit înainte de a putea face vreun rău. Cel mai mare pericol, în afară de pericolul unui antivirus care lasă virusul să treacă din greșeală, este să nu vă dați seama că ați riscat o infecție care ar putea compromite funcționarea PC-ului dumneavoastră sau integritatea datelor dumneavoastră. Tocmai din cauza lipsei de atenție din partea multor persoane, virușii ransomware, cum ar fi Cryptlocker, care criptează fișiere personale și cer răscumpărare, s-au răspândit pe scară largă în ultimul an.

Știm care sunt site-urile periculoase, în general cele care se ocupă de piraterie, site-uri de streaming, conținut pentru adulți, întâlniri și materiale ilegale. Dacă nu puteți evita să vizitați aceste tipuri de site-uri, fiți foarte atenți unde faceți clic, deoarece virusul se poate ascunde oriunde. Este suficient să faceți clic pe butonul greșit de "Download" pentru a ajunge să instalați programe malware. Și nu uitați de acele bannere publicitare care vă spun că PC-ul dumneavoastră este infectat, când de fapt nu este așa.

Dacă aveți îndoieli, există instrumente care vă permit să recunoașteți și să evitați linkurile periculoase și site-urile suspecte.

Un factor cheie în recunoașterea și evitarea site-urilor cu viruși este utilizarea unui browser actualizat, care să fie protejat împotriva tuturor virușilor descoperiți până în prezent.

Printre cele mai periculoase site-uri care pot conține programe malware se numără cu siguranță site-urile pentru adulți, site-urile de piraterie de orice fel, aproape toate site-urile torrent (de asemenea cu piraterie), site-urile de descărcări ilegale (cum ar fi filme și muzică) și site-urile de crack.

În mod ideal, dacă trebuie neapărat să vizitați un astfel de site, cel mai bine ar fi să navigați folosind un sandbox. Atât în Windows 10, cât și în Windows 11 puteți utiliza o funcție de desktop virtual care nu este doar un instrument de securitate, ci și o modalitate excelentă de a face lucruri pe computer fără ca acestea să fie înregistrate sau reținute, un pic ca modul incognito al browserelor web. Acest instrument se numește Sandbox și este conceput ca o zonă a computerului în care tot ceea ce se face nu are nicio influență asupra sistemului și este șters imediat după închiderea acestuia. SandBox funcționează ca o mașină virtuală de unică folosință în

care puteți rula în siguranță tot ce doriți; puteți chiar să deschideți un virus sau un program malware fără să vă faceți griji că acesta vă va deteriora PC-ul sau va fura date din computer.

2) **Confidențialitatea online este mereu în pericol**

Este destul de evident că, dacă doriți să folosiți internetul într-un mod participativ, adică să vă alăturați forumurilor, rețelelor sociale și chat-urilor, trebuie să vă sacrificați o parte din intimitate. Pe site-uri precum Facebook, este obligatoriu să vă dați numele real, în timp ce pe alte site-uri este încă necesar să lăsați o adresă de e-mail prin care, dacă doriți, puteți da de urma proprietarului. Practic, în utilizarea normală a internetului, anonimatul nu poate exista, iar dacă cineva ar fi interesat să afle cine suntem și ar avea abilitățile și talentul de hacking potrivite, ar putea, teoretic, să știe totul despre noi.

Cu toate acestea, protejarea intimității online nu înseamnă să împiedicăm un hacker să ne spioneze viețile, deoarece, cu excepția cazului în care suntem urmăriți de un hărțuitor sau facem lucruri ilegale și care trebuie ascunse, să spunem doar că nimeni nu este probabil să își piardă timpul hackerind viețile noastre. Confidențialitatea online, pe de altă parte, înseamnă păstrarea unor informații sensibile private, cum ar fi numerele cărților noastre de credit, parolele noastre, locul în care ne aflăm la un moment dat, ceea ce căutăm pe internet și așa mai departe.

3) **Site-uri neprotejate**

Acesta este un factor de pericol care este încă ignorat de majoritatea oamenilor.

Site-urile web nu sunt toate la fel și se împart în site-uri securizate, unde informațiile pe care le transmiteți sunt criptate și nu pot fi interceptate din exterior, și site-uri normale, care transmit în clar. Navigaweb.net este în prezent un site necriptat, ceea ce nu înseamnă că nu este securizat, dar pentru că nu necesită o parolă pentru a se conecta, nu are nevoie să protejeze informațiile. Toate site-urile pe care trebuie să introduceți o parolă trebuie să fie criptate, iar această protecție este recunoscută prin lacătul de pe adresa de internet și prin prefixul https în loc de http. Atunci când un site este în HTTPS și nu are erori de certificat, atunci toate informațiile pe care le trimitem, inclusiv parolele de acces, numerele de card de credit sau de cont bancar, nu sunt vizibile pe internet pentru nimeni, nici măcar pentru operatorul site-ului căruia îi trimitem aceste informații. Este de la sine înțeles că pe toate site-urile cu http și fără https nu trebuie să împărtășiți informații personale.

Dacă încă mai folosiți un serviciu de e-mail fără https sau un serviciu bancar online atât de superficial, schimbați neapărat imediat.

4) Phishing

Dintre site-urile periculoase în general, o categorie specială este cea a site-urilor de înșelăciune, cum ar fi site-urile de cumpărături necunoscute și nerecomandate sau, mai rău, site-urile false care arată identic cu site-uri celebre și sunt create pentru a fura parolele conturilor.

Realizarea de site-uri false, copii ale unor site-uri bancare sau de cumpărături, este una dintre cele mai frecvente tehnici folosite de hackeri pentru a fura parolele conturilor web și se numește Phishing. Phishing-ul funcționează întotdeauna prin trimiterea unui mesaj prin e-mail, Facebook, SMS, Whatsapp, etc. Cel mai bun mod de a nu cădea în plasa acestei tehnici este să o folosiți ca scuză pentru a fura parolele. Cel mai bun mod de a nu cădea în acest tip de capcană este să nu scrieți niciodată parolele și datele importante (chiar și prin e-mail) decât pe site-urile oficiale ale conturilor, recognoscibile după adresa scrisă în partea de sus a browserului și HTTPS cu lacăt verde.

În mod ideal, ar fi mai bine să folosiți un client de e-mail, cum ar fi Microsoft Outlook, și să folosiți un filtru de spam pentru a bloca aceste mesaje.

5) Spam

Pericolul spam-ului este mult mai mic în prezent decât era acum câțiva ani.

Spam-ul ar fi întreaga categorie de mesaje nedorite, publicitate, phishing și viruși sau comunicări inutile. Din fericire, serviciile de e-mail de top din ziua de azi, cum ar fi Gmail și Outlook.com, dispun de un filtru de spam eficient care reglează primirea de e-mailuri.

6) Dezinformarea

Deși poate face parte din categoria Spam, dezinformarea pe internet a devenit un pericol real în ultimul an din cauza răspândirii știrilor false de pe site-urile de păcănele, pe care trebuie să învățăm să le recunoaștem pentru a nu părea niște imbecili care cred tot ce citesc pe internet sau pe Facebook.

7) Întâlniri online

Acesta este unul dintre cele mai grave pericole ale internetului pentru tineri.

Sună urât de spus, dar un părinte responsabil ar trebui să verifice dacă copiii săi discută cu străini pe internet, indiferent de circumstanțe. Puteți discuta cu un străin într-un joc online, pe un site de întâlniri ocazionale, pe o rețea de socializare, pe un forum sau în orice altă cameră de chat. Indiferent dacă este vorba de sex, întâlniri sau din motive pur recreative, este important să nu oferiți prea multe informații personale: nu vă spuneți vârsta reală, nu spuneți unde locuiți, nu spuneți la ce școală mergeți, nu dați numele reale ale familiei sau prietenilor și nu dați numărul de telefon. Prădătorii online se pricep foarte bine să se dea drept copii normali și știu cum să exploateze slăbiciunile adolescenților cum nu știu nici cei mai buni psihologi, mânați, în cele mai grave cazuri, de acea boală teribilă care este pedofilia.

8) Cyberbullying

Conversația cu persoane necunoscute poate fi periculoasă, deoarece nu știi niciodată cine se află în spatele tastaturii, dar și conversațiile sau mesajele cu persoane cunoscute pot fi periculoase. Hărțuirea cibernetică funcționează mai mult sau mai puțin în felul următor: dacă ești tachinat la școală sau de către prietenii tăi, unul dintre ei poate posta un videoclip sau o fotografie pe Facebook sau pe alte rețele de socializare care poate pune victima într-o situație jenantă.

Un alt caz de hărțuire cibernetică poate veni din partea unor mesaje anonime care jignesc puternic victima chiar și cu amenințări.

În comparație cu bătăușul real, hărțuitorul cibernetic are avantajul că nu există niciun control și că poate spune tot ce vrea fără să-și privească victima în față sau chiar anonim, ascunzându-se în spatele tastaturii. În ambele cazuri, nu ar fi atât de dificil, cel puțin la nivel tehnic. Este mult mai complicat, însă, să te aperi la nivel psihologic, ceea ce poate necesita ajutorul unui părinte sau al unui expert.

Pentru început, însă, ar fi un excelent pas înainte să ștergeți contul de pe Ask.fm, unul dintre site-urile care se pretează cel mai mult la cyberbullying online.

9) Ignorarea totală a securității informatice

Acesta este un pericol evident, atât de răspândit încât ne surprinde.

Este posibil ca și astăzi cea mai răspândită parolă din lume să fie 123456?

Oare oamenii cred că, pentru că nu au nimic de ascuns, niciun hacker nu le va fura contul?

Cum se poate ca oamenii să folosească în continuare aceeași parolă pentru fiecare site web?

Și mai sunt încă cei care își scriu parolele, poate toate diferite și greu de reținut, pe o bucată de hârtie care poate fi città de oricine?

Acest proiect a fost finanțat cu sprijinul Comisiei Europene. Acest document reflectă doar punctul de vedere al partenerilor de proiect, iar Comisia nu poate fi trasă la răspundere pentru orice utilizare a informațiilor conținute în el.