NEWSLETTER 1

SECURITATE A PROPRIILOR DISPOZITIVE: CALCULATOR, TABLETĂ ȘI TELEFON MOBIL

Subiectul securității pe internet poate fi împărțit în patru părți: protecția dispozitivelor și a rețelei de acasă, parolele, browserele, navigarea pe rețelele wifi.

Pentru fiecare dintre aceste categorii, vom examina tot ceea ce trebuie făcut pentru a atinge un nivel minim de securitate până când sistemul și toate datele transferate pe web și în rețea sunt complet protejate.

Securitatea calculatorului, a tabletei sau a telefonului mobil

Este instalat un antivirus? Antivirusul se actualizează automat în fiecare zi?

Dacă nu ați instalat încă un program antivirus sau dacă aveți un program expirat care nu se mai actualizează, trebuie să luați măsuri.

Dezinstalati antivirusul actual și descărcați unul dintre programele antivirus gratuite recomandate. Pentru a judeca un antivirus într-un mod pe înțelesul tuturor, trebuie să luăm în considerare cel puțin 6 parametri înainte de a lua orice decizie. De fapt, un antivirus bun.

- Nu trebuie să încetinească prea mult PC-ul și să fie ușor în memoria RAM.

- Trebuie să oprească virușii înainte ca aceștia să poată acționa (scanare activă rezidentă).

- Nu trebuie să detecteze prea multe falsuri pozitive, văzând amenințări acolo unde nu există.

- Nu trebuie să facă ca scanarea la cerere sau scanarea automată periodică să dureze prea mult: un SSD modern trebuie să fie scanat complet în mai puțin de 2 ore.

- Trebuie să se actualizeze automat, astfel încât să poată opri imediat noile infecții și să împiedice accesul la părți vitale ale sistemului.

- Trebuie să fie capabil să blocheze programele malware nedescoperite (amenințări 0-day), sesizând amenințarea doar prin comportamentul suspect al anumitor componente.

Pe lângă acești parametri, care sunt toți foarte importanți în materie de antivirus, trebuie să luăm în considerare și ușurința de utilizare, interfața cu utilizatorul, eventualele probleme de utilizare și prezența de bug-uri, erori și incompatibilități.

- Este instalat un firewall?

Dacă aveți Windows 7 și dacă navigați pe internet folosind un router acasă, nu aveți nevoie de un program firewall. Dacă aveți nevoie de unul, puteți descărca un firewall gratuit pentru a vă proteja rețeaua și a bloca intruziunile.

- Este Windows (sau Mac) actualizat și se actualizează automat și regulat?

Mulți oameni neglijează sau uită să actualizeze Windows cu patch-urile pe care Microsoft le distribuie în fiecare săptămână. Aceste actualizări sunt întotdeauna patch-uri de securitate care acoperă cele mai recente găuri care permit utilizatorilor rău intenționați să pătrundă în PC-uri din exterior și să preia controlul.

Verificați dacă serviciul Windows Update este activ în panoul de control.

Nici utilizatorii de Mac nu ar trebui să subestimeze actualizările de securitate.

Ați stabilit un plan de backup pentru datele, documentele și fotografiile dumneavoastră?

Pentru a vă asigura că nu pierdeți fișierele pe care le creați și le salvați pe computer, planificați o copie de rezervă automată a acestora, astfel încât să aveți o copie de rezervă dublă.

Dacă nu aveți prea multe date de salvat, poate fi mult mai ușor și mai rapid să faceți o copie de rezervă online pe servicii de stocare în cloud, cum ar fi Dropbox și Skydrive.

- Păstrați programele instalate pe computerul dumneavoastră la zi?

La fel ca în cazul Windows, se lansează adesea actualizări de securitate pentru programe.

Pentru cei care doresc, există modalități de a actualiza automat programele și software-ul instalat pe computer.

- Atunci când descărcați programe, aveți grijă ca în procedura de instalare să nu instalați și alte programe "recomandate"?

Din păcate, multe programe gratuite sunt însoțite de sponsori, așa-numitele "crapware", sub forma unor programe nesolicitate care se instalează automat.

2) Securitatea browserului

Faptul că computerul, tableta sau telefonul mobil este protejat împotriva virușilor și a intruziunilor externe nu garantează că navigarea este în continuare sigură și privată. Este posibil ca multor persoane să nu le pese de confidențialitate, dar securitatea este totuși primordială.

Indiferent de browserul pe care îl folosiți, acesta ar trebui să fie actualizat la cea mai recentă versiune și să aibă activate actualizările automate. Browserele care sunt la zi și au actualizări automate sunt cu siguranță Chrome, Firefox, Opera și Microsoft Edge.

- Atunci când vă conectați cu o parolă la un site, verificați întotdeauna dacă adresa începe cu https?

HTPPS este protocolul de conexiune criptată și diferă de http normal prin faptul că orice date transmise în https sunt criptate. Acest lucru înseamnă că ceea ce este scris în https este ilizibil pentru oricine, inclusiv pentru operatorii site-ului respectiv.

Extensia de browser HTTPS Everywhere evidențiază site-urile securizate și vă asigură că rămâneți întotdeauna în HTTPS acolo unde este disponibil (a se vedea articolul Navigarea în https pe site-uri bancare, magazine online, Facebook cu o conexiune securizată).

Puteți recunoaște cu ochiul liber site-urile periculoase pe care trebuie să fiți atenți unde faceți clic?

Dacă tot nu puteți deosebi un site bun de unul rău cu ochiul liber și sunteți mereu paranoic sau rău intenționat cu privire la orice alt site în afară de cele mai populare, atunci puteți instala câteva extensii precum WOT pentru a evita să dați click pe link-uri periculoase și site-uri suspecte.

- Atunci când vă conectați la un site de pe un computer care nu este folosit numai de dumneavoastră, vă deconectați întotdeauna?

Nu uitați să vă deconectați întotdeauna de la toate conturile pe care le utilizați pe un computer public sau pe unul partajat cu alte persoane, inclusiv cu membrii familiei.

- Cunoașteți elementele de bază ale escrocheriilor și fraudelor online?

Cunoașterea phishing-ului, a programelor malware și a altor pericole de pe internet este importantă pentru a vă feri de ele.

- Vă protejați browserul de urmărirea online?

După cum s-a explicat deja, a nu fi urmărit online de către site-urile web înseamnă a bloca colectarea de date. Acest lucru este posibil prin intermediul anumitor extensii pe care le puteți instala în browserul dumneavoastră.

Cel mai înalt nivel de protecție și confidențialitate pe internet este navigarea anonimă. Navigarea complet anonimă nu este utilă pentru toată lumea și nu poate fi realizată pentru orice situație. Poate fi util atunci când faceți ceva ilegal (dar bun, cum ar fi descărcarea de torrente), când nu doriți să vă comunicați locația geografică sau când doriți să vă falsificați adresa IP pentru a accesa site-uri blocate.

Deși puteți naviga pe internet în mod anonim în mai multe moduri, confidențialitatea online este garantată doar cu browserul TOR.

Securitatea parolelor folosite online

- Folosiți parole complexe?

Una dintre cele mai frecvente greșeli pe care le fac utilizatorii de internet este aceea de a folosi parole simple sau parole care se referă la fapte sau evenimente din viața lor personală. Ar trebui să alegeți întotdeauna parole imposibil de descoperit și, mai ales, să generați o parolă puternică pentru toate site-urile web, fără a da nimănui șansa de a o ghici (nu folosiți niciodată data nașterii, echipa favorită sau numele soției sau al câinelui).

- Folosiți parole diferite pentru fiecare site?

Nu ar trebui să refolosiți niciodată aceeași combinație de e-mail și parolă în mai multe servicii, deoarece, dacă un hacker reușește să intre în acel cont de e-mail, va putea să spargă fără probleme fiecare cont personal.

Utilizați un program pentru a crea și gestiona parolele pentru conturile web.

Acolo unde este posibil (Dropbox, Google, Gmail și Facebook), se poate utiliza autentificarea cu doi factori.

Pentru o protecție suplimentară, asigurați-vă că verificați permisiunile aplicațiilor de pe Facebook și Twitter.

4) Securitatea rețelei

- Rețeaua dvs. WiFi de acasă este protejată cu o cheie WPA2?

Dacă nu, sau dacă nu aveți nicio idee despre ce este WPA2, trebuie să știți că WPA înseamnă Wi-Fi Protected Access și că Wi-Fi Protected Access II (WPA2) și Wi-Fi Protected Access III (WPA3) sunt trei protocoale de securitate și programe de certificare dezvoltate de Wi-Fi Alliance pentru a proteja rețelele de calculatoare fără fir.

- Sunteți conștient de faptul că, atunci când vă conectați la o rețea Wi-Fi deschisă, tot ceea ce faceți este vizibil din afara computerului dumneavoastră?

Singurul lucru care protejează securitatea parolelor pe internet într-o rețea wifi publică este protocolul HTTPS menționat la prima întrebare de la punctul doi.

- Ați verificat folderele partajate de pe computer?

După cum s-a demonstrat, este foarte ușor să pătrunzi în calculatoare și să vizualizezi dosarele partajate ale altor calculatoare. Foarte adesea operațiunea are succes deoarece oamenii uită să excludă partajarea folderelor sau a întregului hard disk de pe computer. Pentru a utiliza un computer în anonimat complet și a vă conecta la rețea fără a lăsa urme, puteți utiliza un sistem Linux anonim și privat, cum ar fi Tails.

Securitatea este importantă pentru toată lumea, de la tehnicianul experimentat până la analfabetul în domeniul calculatoarelor. Nivelul de precauții pe care îl luați depinde de dumneavoastră, dar țineți cont de faptul că, în prezent, securitatea online este la fel de importantă (dacă nu chiar mai importantă) ca și securitatea propriei locuințe.

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.