Sfaturi şi recomandări

Prezentele sfaturi şi recomandări vă ajută să vă faceţi un obicei din navigarea online în condiţii de securitate. Această secţiune a fost elaborată în coordonare cu serviciul guvernamental de securitate Get Safe Online din Regatul Unit şi Departamentul de Securitate Naţională (Department of Homeland Security) din Statele Unite ale Americii.

- Protejaţi-vă calculatorul personal (PC-ul) şi dispozitivele portabile
- Protejaţi-vă informaţiile cu caracter personal şi identitatea
- Protejaţi informaţiile cu caracter comercial în afara organizaţiei dumneavoastră
- Atenţie în momentul conectării
- Navigaţi inteligent pe internet

Protejaţi-vă calculatorul personal (PC-ul) şi dispozitivele portabile

PC

- Utilizaţi un paravan de protecţie: paravanele de protecţie vă protejează reţeaua împotriva unor viruşi şi a hackerilor
- Instalaţi un program antivirus: programele antivirus previn răspândirea viruşilor în calculatorul dumneavoastră
- Efectuaţi în permanenţă actualizările de securitate: menţineţi aplicaţiile şi sistemul de operare în stare bună de funcţionare, fără probleme şi în permanenţă actualizate
- Nu permiteţi accesul programelor spion: nu permiteţi accesul persoanelor străine în calculatorul dumneavoastră evitând e-mail-urile şi ataşamentele suspecte
- Creaţi periodic copii de rezervă: protejaţi-vă datele în caz de defectare a sistemului

Laptop-uri

- Închideţi conexiunile wireless atunci când nu sunt utilizate sau necesare
- Conectaţi-vă în mod periodic laptopul la o reţea de încredere pentru a vă actualiza mecanismele de securitate.
- Creaţi copii de rezervă ale informaţiilor stocate pe laptopul dumneavoastră
- Nu lăsaţi laptopul dumneavoastră nesupravegheat

Unităţi USB

- Utilizaţi o unitate USB criptată
- Activaţi modul exclusiv pentru citire utilizând comutatorul fizic, pentru a evita transmiterea viruşilor: unele unităţi USB includ un comutator fizic pentru activarea modului exclusiv

pentru citire pentru a împiedica scrierea sau modificarea de pe calculatorul gazdă a datelor din unitatea USB

- Scanaţi unitatea USB după copierea fişierelor dintr-un echipament care nu este de încredere sau care nu este autorizat, pentru a evita transmiterea viruşilor
- Înainte de a introduce unitatea dumneavoastră USB în calculatorul unei alte persoane, ştergeţi toate fişierele care nu sunt relevante în scopul acţiunii respective
- Creaţi copii de rezervă ale informaţiilor de pe unitatea dumneavoastră USB pentru a recupera datele în cazul unei defectări
- Ataşaţi unităţile USB la brelocuri sau şnururi tip portecuson pentru a evita pierderea acestora: din cauza dimensiunii reduse a unităţilor USB, acestea pot fi pierdute sau furate cu uşurinţă. În plus, cu cât este mai mare capacitatea lor de stocare, cu atât este mai mare cantitatea de date expuse riscului de acces neautorizat. Unităţile USB sunt de obicei ţinute în genţi, rucsacuri, huse pentru laptop, jachete, buzunarele pantalonilor sau sunt lăsate în staţii de lucru nesupravegheate. Numărul incidentelor a crescut recent, unităţile USB fiind pierdute, rătăcite, împrumutate fără permisiune sau furate

Telefoanele mobile şi calculatoarele portabile

Calculatoarele portabile precum dispozitivele Windows Mobile, Palm, iPhone, Android şi Blackberry pot fi conectate la internet şi au capacitatea de a stoca o foarte mare cantitate de informaţii. Chiar faptul că sunt portabile înseamnă că trebuie să fie tratate cu deosebită atenţie

- Închideţi conexiunile wireless (şi anume, Bluetooth şi WLAN) atunci când acestea nu sunt utilizate. Tehnologia Bluetooth permite comunicarea între dispozitivele electronice prin utilizarea unei legături radio cu rază scurtă
- Nu vă lăsaţi telefonul mobil şi calculatorul portabil nesupravegheate. În caz contrar, aţi putea suferi pierderi de date
- Utilizaţi funcţia de creare a parolei pentru a preveni accesul neautorizat de la distanţă în telefonul dumneavoastră

Protejaţi-vă informaţiile cu caracter personal şi identitatea

- **Utilizaţi o parolă sigură**: parola dumneavoastră este echivalentul pe internet al yalei şi cheii de la locuinţă. Parolele reprezintă un mecanism important de apărare iar dezvoltarea unor bune practici în ceea ce priveşte parolele vă va ajuta să vă păstraţi în mai mare siguranţă informaţiile cu caracter personal şi identitatea. Parola calculatorului dumneavoastră este cheia de acces la toate informaţiile – atât profesionale, cât şi personale – pe care le-aţi stocat în calculatorul dumneavoastră şi în conturile dumneavoastră online. Utilizaţi o parolă sigură pentru a vă proteja datele: utilizaţi un set complex de caractere; combinaţi litere (majuscule şi minuscule), cifre şi simboluri. Cu cât este mai mare varietatea caracterelor pe care le includeţi în parola dumneavoastră, cu atât aceasta este mai dificil de ghicit. Nu utilizaţi informaţii personale – numele dumneavoastră, al copilului, date de naştere etc. –

pe care alte persoane pot deja să le cunoască sau să le obţină cu uşurinţă şi încercaţi să evitaţi cuvintele comune: unii hackeri utilizează programe care încearcă fiecare cuvânt din dicţionar

- **Schimbaţi-vă frecvent parola**: în cazul în care consideraţi că sistemul dumneavoastră a fost compromis, schimbaţi parolele imediat
- **Păstraţi secretul cu privire la parola dumneavoastră**: parola dumneavoastră este unică şi nu trebuie comunicată nimănui. Ori de câte ori este posibil, încercaţi să reţineţi parolele. Adoptaţi o strategie pentru a le memora. Dacă vă notaţi parola undeva, aveţi grijă unde. Nu lăsaţi astfel de evidenţe ale parolelor dumneavoastră în locuri în care nu aţi lăsa informaţiile pe care acestea le protejează
- **Cont unic, parolă unică**: utilizaţi parole diferite pentru fiecare cont online pe care îl accesaţi (sau cel puţin mai multe parole). Dacă utilizaţi aceleaşi parole la mai multe conturi, un atacator care obţine accesul la un cont va putea avea acces la toate conturile dumneavoastră
- **Securizaţi-vă conturile**: numeroşi furnizori de conturi oferă modalităţi suplimentare pentru a verifica cine sunteţi înainte de a efectua activităţi pe site-ul respectiv
- **Luaţi singur decizii cu privire la prezenţa dumneavoastră online**: atunci când sunt disponibile setări de confidenţialitate şi securitate pe site-uri, configuraţi-le în conformitate cu nivelul de partajare a informaţiilor pe care îl doriţi. Este de preferat să limitaţi numărul persoanelor cu care partajaţi informaţii
- **Utilizaţi cu atenţie site-urile de socializare**: trebuie să ştii că site-urile de socializare pot reuni numeroase riscuri asociate prezenţei online; agresiunile online, divulgarea informaţiilor private, urmărirea informatică, accesul la conţinuturi inadecvate vârstei şi, în cazurile cele mai grave, acostarea copiilor prin intermediul internetului şi abuzurile împotriva acestora

Protejaţi informaţiile cu caracter comercial în afara organizaţiei dumneavoastră

- **Asiguraţi-vă că păstraţi securitatea informaţiilor dumneavoastră sensibile**: atunci când vă aflaţi în afara organizaţiei dumneavoastră, asiguraţi-vă că păstraţi informaţiile sensibile şi echipamentele în condiţii de securitate în permanenţă, pentru a preveni furtul sau pierderea. În special, atunci când vă aflaţi în locuri publice, trataţi informaţiile cu atenţie
- **Păstraţi confidenţialitatea informaţiilor cu caracter comercial**: trebuie să reţineţi că cineva poate auzi conversaţia pe care o purtaţi. Nu divulgaţi oricărei persoane informaţiile confidenţiale ale organizaţiei dumneavoastră
- **Protejaţi-vă împotriva „uitatului peste umăr”**: atunci când călătoriţi sau când lucraţi de la distanţă protejaţi-vă împotriva persoanelor din spatele dumneavoastră care pot observa ce faceţi
- **Utilizaţi în mod inteligent serviciile de webmail**: atunci când utilizaţi un browser pentru a vă citi e-mail-urile trebuie să fiţi la fel de atent ca atunci când utilizaţi un sistem de e-mail de birou, existând anumite riscuri proprii de securitate

Atenţie în momentul conectării

- **Închideţi conexiunile wireless atunci când nu sunt utilizate sau nu sunt necesare**
- **Informaţi-vă cu privire la spaţiile de tip hotspot wi-fi**: Atunci când utilizaţi spaţii de tip hotspot wi-fi, limitaţi activităţile pe care le desfăşuraţi şi ajutaţi setările de securitate pe dispozitivul dumneavoastră pentru a limita numărul persoanelor care pot avea acces la acesta
- **Protejaţi-vă banii**: Atunci când utilizaţi servicii bancare sau faceţi cumpărături online, verificaţi dacă site-urile au mecanisme de securitate. Căutaţi adrese de web cu „https://” sau „shttp://”, ceea ce înseamnă că site-urile respective iau măsuri suplimentare pentru a păstra securitatea informaţiilor dumneavoastră. Http:// nu este sigur
- **Blocaţi e-mail-urile nedorite**: e-mail-urile tip spam reprezintă o ameninţare la adresa securităţii. Nu deschideţi e-mail-urile şi ataşamentele necunoscute
- **Când aveţi îndoieli, ştergeţi elementele suspecte**: Atunci când link-urile din e-mail-uri, tweet-uri, posturi şi anunţuri publicitare online arată suspect, chiar în cazul în care cunoaşteţi sursa, se recomandă să le ştergeţi sau, după caz, să le marcaţi drept corespondenţă nedorită
- **Trimiteţi mai departe e-mail-urile dacă este adecvat.** Aveţi în vedere ştergerea istoricului mesajului înainte de a face acest lucru
- **Navigaţi cu atenţie pe internet**
- **Nu descărcaţi documente şi materiale de la persoane în care nu aveţi încredere**
- **Utilizaţi cu atenţie calculatoarele publice:** Conectaţi-vă la un calculator public doar dacă aveţi o conexiune criptată (indicată de un lacăt în partea dreapta jos a ferestrei browserului şi literele „https://” la începutul adresei site-ului)
- **Utilizaţi servicii de webmail furnizate de companii de renume şi de încredere**

Navigaţi inteligent pe internet

- **Informaţi-vă în permanenţă:** ţineţi pasul cu noile modalităţi de menţinere a securităţii online: accesaţi site-uri de încredere pentru a afla cele mai recente informaţii şi comunicaţi-le familiei, prietenilor şi colegilor şi încurajaţi-i şi pe ei să navigheze inteligent pe internet. Setaţi browserul în aşa fel încât să fie sigur
- **Gândiţi înainte de a acţiona**: aveţi grijă la comunicările care vă sugerează să faceţi ceva pe loc, vă oferă ceva care sună prea bine pentru a fi real sau vă solicită informaţii cu caracter personal
- **Creaţi copii de rezervă**: protejaţi-vă lucrările, muzica, fotografiile şi alte informaţii digitale prin crearea de copii electronice şi stocarea acestora într-un loc sigur