GHID

UTILIZAREA CALCULATORULUI ÎN CONDIȚII DE SIGURANȚĂ ȘI SECURITATE

Ghid realizat de:

Microsoft

CUPRINS

Scopul prezentului document este de a familiariza cititorii cu noțiunile de bază privind tipurile de amenințări informatice, precum și de a propune o serie de practici menite să protejeze sistemul și datele personale, în timpul navigării pe internet.

Utilizarea unui paravan de protecție

Un paravan de protecție este un software sau un hardware care verifică informațiile venite de pe Internet sau dintr-o rețea, apoi fie le îndepărtează, fie le permite să treacă în computer, în funcție de cum ați setat paravanul de protecție. Astfel, un paravan de protecție ajută la împiedicarea hackerilor și a software-ului rău intenționat să aibă acces la computer.

Paravanul de protecție Windows este inclus în Windows și este activat automat.
Ilustrație a modalității de funcționare a unui paravan de protecțieCum funcționează un paravan de protecție

Dacă executați un program, cum ar fi un program de schimb instantaneu de mesaje sau un joc de rețea cu mai mulți jucători care are nevoie să primească informații de pe Internet sau dintr-o rețea, paravanul de protecție vă întreabă dacă blocați sau deblocați (permiteți) conexiunea. Dacă alegeți deblocarea conexiunii, Paravanul de protecție Windows creează o excepție pentru ca paravanul de protecție să nu vă deranjeze în viitor atunci când acel program are nevoie să primească informații.

Utilizarea protecției antivirus

Virușii, viermii și caii troieni sunt programe create de hackeri, care utilizează Internetul pentru a infecta computere vulnerabile. Virușii și viermii se pot reproduce de la computer la computer, în timp ce caii troieni intră într-un computer ascunzându-se într-un program aparent legitim, cum ar fi un economizor de ecran. Virușii, viermii și caii troieni destructivi pot să șteargă informații din hard disk sau să dezactiveze complet computerul. Alții nu cauzează daune directe, dar înrăutățesc performanța și stabilitatea computerului.

Programele antivirus scanează mesajele electronice și alte fișiere de pe computer pentru detectarea virușilor, viermilor și cailor troieni. Dacă este găsit unul, programul antivirus fie îl pune în carantină (izolează), fie îl șterge în întregime înainte de a deteriora computerul și fișierele.

Windows nu are un program antivirus inclus, dar este posibil ca producătorul de computere să fi instalat unul. Dacă nu, sunt multe programe antivirus disponibile. Microsoft oferă Microsoft Security Essentials, un program antivirus gratuit ce poate fi descărcat de la site-ul Web Microsoft Security Essentials. De asemenea, puteți accesa site-ul Web Furnizori de software de securitate Windows 7 pentru a găsi un program antivirus de la terți.

Deoarece în fiecare zi sunt identificați noi viruși, este important să utilizați un program antivirus cu capacitate de actualizare automată. Atunci când programul este actualizat, acesta adaugă virușii noi în lista de viruși, pe care îi caută, ajutând la protejarea computerului de noi atacuri. Dacă lista de viruși este depășită, computerul este vulnerabil la amenințări noi. Actualizările cer de obicei o taxă anuală de abonare. Păstrați permanent abonarea pentru a primi actualizări regulate.
Avertisment

Dacă nu utilizați un software antivirus, expuneți computerul la deteriorare din cauza software-ului rău intenționat. De asemenea, vă asumați riscul de a răspândi viruși în alte computere.

Utilizarea protecției antispyware

Programele spion sunt acele tipuri de software care pot să afișeze reclame, să colecteze informații despre dvs. sau să modifice setările din computer, de obicei fără a avea aprobarea dvs. De exemplu, programele spion pot să instaleze bare de instrumente nedorite, linkuri sau preferințe în browserul Web, pot să modifice pagina de pornire implicită sau să afișeze frecvent reclame pop-up. Unele programe spion nu afișează niciun indiciu pentru a le detecta, dar colectează în secret informații sensibile, cum ar fi site-urile Web pe care le vizitați sau textul pe care îl tastați. Majoritatea programelor spion sunt instalate prin intermediul unui software gratuit pe care îl descărcați, dar în unele cazuri simpla vizitare a unui site Web poate duce la o infectare cu programe spion.

Pentru a ajuta la protejarea computerului de programe spion, utilizați un program antispyware. Această versiune de Windows are un program antispyware inclus, denumit Windows Defender, care este activat implicit. Windows Defender vă avertizează atunci când un program spion încearcă să se auto-instaleze pe computer. De asemenea, acesta poate să scaneze computerul în căutare de programe spion existente, eliminându-le apoi.

Deoarece în fiecare zi apar noi tipuri de programe spion, Windows Defender trebuie actualizat în mod regulat pentru a detecta și a vă apăra de cele mai noi amenințări. Windows Defender este actualizat după cum este necesar, atunci când actualizați Windows. Pentru nivelul cel mai ridicat de protecție, setați Windows să instaleze automat actualizările (vedeți mai jos).

Actualizați automat Windows

Microsoft oferă în mod regulat actualizări automate importante pentru Windows, care ajută la protejarea computerului în fața virușilor noi și a altor amenințări la adresa securității. Pentru a

vă asigura că primiți aceste actualizări cât mai repede posibil, activați actualizarea automată. Astfel, nu trebuie să vă îngrijorați că de pe computer lipsesc remedieri critice pentru Windows.

Actualizările se descărcă „în spatele scenei”, atunci când sunteți conectat la Internet. Actualizările se instalează la ora 3:00 AM, în cazul în care nu specificați o altă oră. Dacă închideți computerul înainte de acest moment, instalați actualizări înainte de a închide computerul. Altfel, Windows le va instala la următoarea deschidere a computerului.

Pentru a activa actualizarea automată

1. Deschideți Windows Update făcând clic pe butonul Start. În caseta de căutare, tastați update, apoi, în lista cu rezultate, faceți clic pe Windows Update.
2. Faceți clic pe Modificare setări.
3. Asigurați-vă că Se instalează actualizările automat (recomandat) este bifată.

   Windows va instala actualizările importante pentru computer dvs. pe măsură acestea devin disponibile. Actualizările importante oferă beneficii semnificative, cum ar fi securitatea și fiabilitatea îmbunătățite.

4. Sub Actualizări recomandate, bifați caseta de selectare Se primesc actualizările recomandate în același mod în care se primesc și actualizările importante, apoi faceți clic pe OK.

   Actualizările recomandate se adresează problemelor mai puțin importante și pot contribui la îmbunătățirea experienței cu computerul. Dacă vi se solicită o parolă de administrator sau o confirmare, tastați parola sau furnizați confirmarea.

Instalați cea mai recentă versiune a browserului Web și păstrați-o la zi

Cele mai bune două metode de a împiedica probleme online sunt următoarele: utilizarea celei mai recente versiuni de browser și actualizarea browserului. În majoritatea cazurilor, cea mai recentă versiune de browser conține remedieri de securitate și caracteristici noi care pot contribui la protejarea computerului și a confidențialității dvs., cât timp sunteți online.

De asemenea, multe browsere Web oferă periodic actualizări de securitate. Deci, asigurați-vă că instalați actualizări pentru browser ori de câte ori acestea devin disponibile.

Dacă aveți Internet Explorer, este posibil să obțineți automat actualizări pentru acesta, utilizând Windows Update. În cazul în care computerul nu este configurat pentru a primi automat actualizări, aveți posibilitatea să solicitați manual aceste actualizări, utilizând Internet Explorer. Faceți clic pe butonul Siguranță, apoi faceți clic pe Windows Update. Urmați instrucțiunile de pe ecran pentru a căuta actualizări.

Activați caracteristicile de securitate din browser

Multe browsere Web dețin caracteristici de securitate care vă ajută să navigați pe Web în siguranță. Este o idee bună să aflați ce caracteristici de securitate are browserul dvs. și să vă asigurați că sunt activate.

Dacă aveți Internet Explorer, iată câteva dintre caracteristicile de securitate care sunt disponibile:

- Filtrul SmartScreen, care vă poate ajuta să vă protejați de atacurile de înșelăciune online, de frauda online și de site-uri Web false sau răuvoitoare. Pentru mai multe informații, consultați Filtrul SmartScreen: întrebări frecvente.

- Evidențierea domeniului, care vă permite să vedeți mult mai ușor adresa Web reală a site-urilor Web vizitate. Aceasta vă ajută să evitați site-urile Web înșelătoare sau impostoare care utilizează adrese Web ce induc în eroare pentru a vă amăgi. Domeniul adevărat pe care îl vizitați este evidențiat în bara de adrese.

- Gestionare programe de completare, care vă permite să dezactivați sau să permiteți programe de completare ale browserului Web și să ștergeți controalele ActiveX nedorite. Pentru mai multe informații, consultați Cum influențează computerul programele de completare ale browserului?

- Filtrul XSS (Cross site scripting), care vă poate ajuta să preveniți atacurile din partea site-urilor Web înșelătoare sau frauduloase care pot încerca să vă fure informații personale și financiare. Pentru mai multe informații, consultați Cum mă ajută Internet Explorer să mă protejez de atacurile cu scripturi între site-uri?

- O conexiune pe 128 biți securizată (SSL) pentru utilizarea site-urilor Web sigure. Aceasta ajută Internet Explorer să creeze o conexiune criptată cu site-urile Web furnizate de bănci, magazine online, site-uri medicale sau alte organizații care gestionează informații sensibile despre clienți. Pentru mai multe informații, consultați Cum pot ști dacă o tranzacție online este securizată.

Pentru mai multe informații despre protejarea computerului și confidențialitatea online, accesați site-ul Web Microsoft Security sau site-ul Web Microsoft Online Safety.
Începutul paginii

Utilizarea unui cont de utilizator standard

Atunci când vă faceți log on la computer, Windows vă acordă un anumit nivel de drepturi și privilegii, în funcție de tipul de cont de utilizator deținut. Există trei tipuri diferite de conturi de utilizator: standard, administrator și vizitator.

Deși un cont de administrator oferă un control complet asupra unui computer, utilizarea unui cont standard vă poate ajuta să faceți computerul mai sigur. Astfel, dacă alte persoane (sau hackeri) obțin acces la computer atunci când ați făcut log on, aceștia nu au posibilitatea să deschidă setările de securitate ale computerului sau să modifice conturile altor utilizatori. După ce faceți logon, aveți posibilitatea să verificați tipul de cont efectuând următoarele:

Pașii de urmat vor varia în funcție de situarea computerului, într-un domeniu sau într-un grup de lucru. Pentru a afla, consultați „Pentru a afla dacă computerul dvs. este într-un grup de lucru sau un domeniu“ din Care este diferența dintre un domeniu, un grup de lucru și un grup de domiciliu?

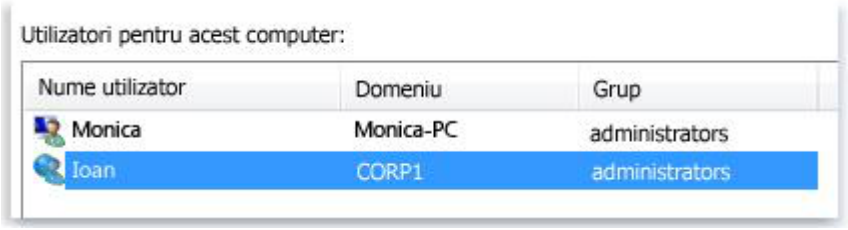
Computerul este într-un domeniu

1. Tastați numele de utilizator și parola pentru cont în ecranul Bun venit.

Ecranul Bun venit

2. Pentru a deschide Conturi de utilizator, faceți clic pe butonul Start, pe Panou de control, pe Conturi de utilizator, faceți clic pe Conturi de utilizator, apoi faceți clic pe Gestionare conturi de utilizator. Dacă vi se solicită o parolă de administrator sau o confirmare, tastați parola sau furnizați confirmarea.

   Numele dvs. de utilizator este evidențiat, iar tipul dvs. de cont este afișat în coloana Grup.



Utilizatorul înregistrat în prezent și tipul de cont al utilizatorului

Computerul este într-un grup de lucru

1. Tastați numele de utilizator și parola pentru cont în ecranul Bun venit.

Ecranul Bun venit

2. Pentru a deschide Conturi de utilizator, faceți clic pe butonul Start, pe Panou de control, pe Conturi de utilizator și siguranța familiei, faceți clic pe Conturi de utilizator, apoi faceți clic pe Gestionează alt cont. Dacă vi se solicită o parolă de administrator sau o confirmare, tastați parola sau furnizați confirmarea.

   Tipul dvs. de cont este afișat sub numele de utilizator.

Utilizatorul înregistrat în prezent și tipul de cont al utilizatorului

Dacă tipul dvs. de utilizator este Administrator, atunci sunteți înregistrat în prezent ca administrator.

Dacă utilizați în mod curent un cont de administrator, consultați Modificarea tipului de cont al unui utilizator pentru a învăța cum să îl transformați într-un cont standard.

Sfaturi pentru utilizarea în siguranță a poștei electronice și a Webului

Fiți precauți atunci când deschideți atașări de poștă electronică. Atașările de poștă electronică (fișiere atașate mesajelor de poștă electronică) sunt o sursă principală de infectare cu viruși. Nu deschideți niciodată o atașare primită de la o persoană necunoscută. În cazul în care cunoașteți expeditorul, dar nu așteptați o atașare, verificați dacă expeditorul chiar v-a trimis atașarea, înainte de a o deschide.

Păstrați cu grijă informațiile personale. Dacă un site Web vă cere un număr de carte de credit, informații bancare sau alte informații personale, asigurați-vă că site-ul Web este de încredere și verificați dacă sistemul său de tranzacție este unul sigur.

Fiți atenți atunci când faceți clic pe hyperlinkuri în mesaje de poștă electronică. Hyperlinkurile (legături care deschid site-uri Web atunci când faceți clic pe acestea) sunt utilizate adesea în cadrul unor trucuri pentru înșelătorie sau programe spion, dar pot transmite și viruși. Faceți clic numai pe linkurile din mesajele de poștă electronică în care aveți încredere.

Instalați programe de completare numai din site-uri Web în care aveți încredere. Programele de completare pentru browserul Web permit paginilor Web să afișeze elemente cu ar fi bare de instrumente, cotații bursiere, clipuri video și animație. Totuși, programele de completare pot instala și un program spion sau alt software rău intenționat. Dacă un site Web vă cere să instalați un program de completare, asigurați-vă că site-ul este de încredere înainte de a face acest lucru.