Ghid pentru certificarea IC3 GS5

Lecția 7: Securitate și Mentenanță

Obiectivele lecției

- explică nevoia de securitate
- descrie cum să păstrezi în siguranță numele tău de utilizator și parola
- descrie riscurile prezentate de viruși, viermi, Trojan și malware
- descrie riscurile asociate conexiunilor la rețea
- protejarea informației personale când utilizezi computere publice
- descrie riscurile prezentate de ingineria socială și atacurile de tip phishing
- descrie metodele de protecție împotriva producerii riscurilor
- explică cum și de ce facem backup și restaurarea informațiilor și a setărilor
- explică cum resetăm dispozitivele personale la setările lor de fabrică
- descrie tehnicile de bază de depanare
- înțelege tehnicile de bază de depanare

Nevoia de securitate

- Deîndată ce conectezi un computer la o rețea, expui sistemul și informația stocată pe acesta la potențialele riscuri asociate lucrului în rețea
- Informația stocată pe un computer conectat la rețea poate, teoretic, fi accesată de pe oricare computer conectat la rețea
- Dacă rețeaua oferă și acces la internet, riscul creste
- *Hackerii* aplică multe și diverse metode pentru a obține ceea ce doresc
- Trebuie să iei măsuri pentru a-ti proteja computerul și informațiile

Nume de utilizatori și parole

- Numele de utilizator și parola protejează contul tău de un eventual acces neautorizat
- Parolele puternice îți protejează conturile
  - Utilizează cel puțin șase caractere; opt sau mai multe, cincisprezece fiind considerat cel mai înalt nivel de securitate
  - Combină numere, litere, simboluri și litere majuscule
  - Alege una ușor de memorizat, dar dificil de ghicit pentru altcineva
  - Evită să utilizezi numele persoanelor apropiate
  - Evită să utilizezi variațiuni ale numelui tău sau să incluzi numele, adresa sau data nașterii tale
  - Evită să utilizezi variațiuni de parole ușor de ghicit

Nume de utilizatori și parole

- **Păstrarea conturilor tale în siguranță**
  - Contul tău îți protejează fișierele și reputația
    - Niciodată nu partaja informațiile contului tău
    - Dacă ai partajat întâmplător informațiile tale de autentificare, modifică-le imediat
    - Nu "ascunde" parola ta în proximitatea computerului
    - Nu utiliza aceeași parolă pentru toate conturile tale

Nume de utilizatori și parole

- **Schimbarea parolei**
  - Pentru a modifica parola ta de Windows 10:
    1. Accesează **Start**, apoi **Setări**
    2. Fă clic pe **Conturi**, apoi **Opțiuni de conectare**
    3. Sub *Parolă*, apasă pe **Modificare**
    4. Introdu parola ta veche, apoi fă clic pe **Următorul**
    5. Scrie noua ta parolă, scrie din nou noua ta parolă pentru a confirma, introdu o sugestie pentru parolă, apoi apasă **Următorul**
    6. Fă clic pe **Finalizare**
  - Dacă utilizezi un cont de domeniu, urmează acești pași pentru a modifica parola ta de conectare:
    1. Tastează **Ctrl** + **Alt** + **Delete**
    2. Fă clic pe **Modificare parolă**.
    3. Scrie parola ta veche, scrie noua ta parolă, mai scrie o dată noua parolă pentru a o confirma, apoi apasă **Enter**

Nume de utilizatori și parole

- **Blocarea sistemului**
  - Se recomandă să deconectezi sistemul dacă intenționezi să pleci de lângă computer indiferent de durata absenței tale.
  - Cea mai comodă opțiune este blocarea sistemului cât timp ești plecat
  - Când blochezi sistemul, toate programele și fișierele rămân deschise și gata să-ti poți relua rapid munca
  - Pentru a bloca sistemul, apasă pe **Start**, fă clic pe pictograma contului tău din colțul de sus din dreapta a meniului Start, apoi fă clic pe **Blocare**

Identificarea Riscurilor

- **Virușii**
  - Un virus este un program malițios conceput să preia controlul asupra operațiunilor sistemului și să deterioreze sau să distrugă informații
  - Virușii pot fi transmiși prin atașări la email, descărcări de programe sau fișiere ori prin utilizarea discurilor infectate, CD-uri sau unități flash
  - Un virus poate:
    - Afișa pe ecran mesaje inofensive
    - Utiliza toată memoria disponibilă, astfel încetinind sau întrerupând celelalte procese
    - Corupe sau distruge fișiere de date
    - Șterge întregul conținut al unității de disk

Identificarea Riscurilor

- **Viermii (En ”Worms”)**
  - Un vierme este un program care se auto-multiplică și care consumă resursele sistemului și ale rețelei
  - Diferența dintre un vierme și un virus este că viermele se răspândește automat de pe un computer pe altul, în timp ce un virus necesită careva acțiuni pentru a fi transmis
  - Un vierme se poate localiza în memoria activă și se poate multiplica în rețea
  - Un *Troian* (En „Trojan”) este un program conceput să acorde unui hacker acces de la distanta la sistemul computerului urmărit
  - Troienii se instalează pe sistemul urmărit când utilizatorul rulează aplicația infectată, permițând-I astfel unui hacker să preia controlul asupra sistemului, să fure informații, să instaleze alt software (inclusiv viruși), să descarce sau să încarce fișiere, ori să blocheze sistemul

Identificarea Riscurilor

- **Malware (Spyware / Adware)**
  - *Spyware* este o aplicație software plasată în mod secret pe sistemul tău cu scopul de a acumula informații personale sau private fără consimțământul sau cunoștința ta
  - *Adware* este o aplicație software care afișează sau descarcă publicitate în mod automat
  - Odată instalat, spyware monitorizează activitatea ta pe Internet și transmite informația către inițiatorul spyware
    - Scanează fișiere de pe unități de discuri
    - Citește cookie-uri
    - Monitorizează intrările de la tastatură
    - Instalează alte aplicații spyware
    - Schimbă pagina implicită de Acasă din browsere Web
    - Expediază în mod automat informații către dezvoltatorul de spyware

Identificarea Riscurilor

- Un cookie este un fișier text de mici dimensiuni inserat în computerul tău de către un server Web
- Cookie-urile pot fi folosite pentru a stoca nume de utilizatori și parole și pentru a urmări activitățile din browser
- Un hacker care deține acces fizic la sistemul tău sau instalează cu succes un spyware poate sustrage cookie-urile tale, iar odată cu acestea, orice nume de utilizator și parole stocate
- Poți instala și descărca programe gratuite spyware/adware sau poți utiliza Windows Defender pentru a-ti monitoriza sistemul

Identificarea Riscurilor

- **Conexiunile la rețea**
  - **Conexiunile cu fir (Ethernet)**
    - La modul general, dacă te conectezi la o rețea cu fir din cadrul școlii sau biroului, ești în siguranță
    - Administratorii de rețea depun mari eforturi pentru a se asigura că toate sistemele companiei/școlii sunt scanate periodic pentru a depista infecții, în plus, toți utilizatorii trebuie să se conecteze la rețea folosind un nume valid de utilizator și o parolă
    - Totuși, aceste măsuri de garantare nu funcționează și în cazul în care te conectezi la o rețea publică cu fir

Identificarea Riscurilor

- **Conexiunile fără fir (Wi-Fi)**
  - Oricine se poate alătura unei rețele Wi-Fi furnizate de un hotspot public
  - Nimeni nu poate garanta că toate sistemele conectate nu au viruși, și că nu există un hacker care pândește din spate așteptând să găsească un sistem pe care să-l exploateze
  - Sistemele fără fir se conectează direct unul la celălalt în cadrul unei rețele ad-hoc; în centru, nu există un punct de acces care să transmită semnalele între participanți, și nu este nevoie de autentificare
- **Diminuarea riscurilor**
  - De fiecare data când te conectezi la o rețea publică, întotdeauna identifică rețeaua în sistemul de operare ca rețea Publică
  - Dacă utilizezi Wi-Fi, întotdeauna, conectează-te la o rețea de infrastructură
  - Evită să te conectezi la rețele ad-hoc

Identificarea Riscurilor

- **Utilizarea Computerelor Publice**
  - **Deconectează conturile online** – dacă te-ai conectat la un cont online, nu pleca fără să-l deconectezi, pentru că oricine care vine după tine poate accesa respectivul cont și poate realiza acțiuni din numele tău, deoarece ești în continuare conectat
  - **Curată cache-urile și cookie-urile** – browserele stochează informații în locații de stocare denumite cache-uri care se află pe unitatea de disc; pentru a-ti menține activitatea online în privat, utilizează caracteristicile incorporate din browserul tău de curățare a acestor intrări
  - **Deconectează sistemul de operare** – dacă folosești un computer partajat la școală sau la serviciu care solicită conectare personală, întotdeauna deconectează când finalizezi lucrul pe computer.

Identificarea Riscurilor

- **Identificarea Riscurilor**
  - *Ingineria socială* reprezintă o practică de înșelare a utilizatorilor ca aceștia să furnizeze parole sau alte tipuri de informații de acces
  - Inginerii sociali se bazează pe dorința oamenilor de a fi de ajutor
  - Inginerii sociali, de asemenea, încearcă să imite utilizatorii legali creând confuzia că ar fi operator de tablou de distribuție sau un gardian de securitate
  - Țintele tipice ale strategiei de inginerie socială includ persoanele care dispun de acces la informații de sistem pe care nu le utilizează, incluzând persoane din secretariat, oameni de serviciu, unii administratori și chiar personalul din securitate

Identificarea Riscurilor

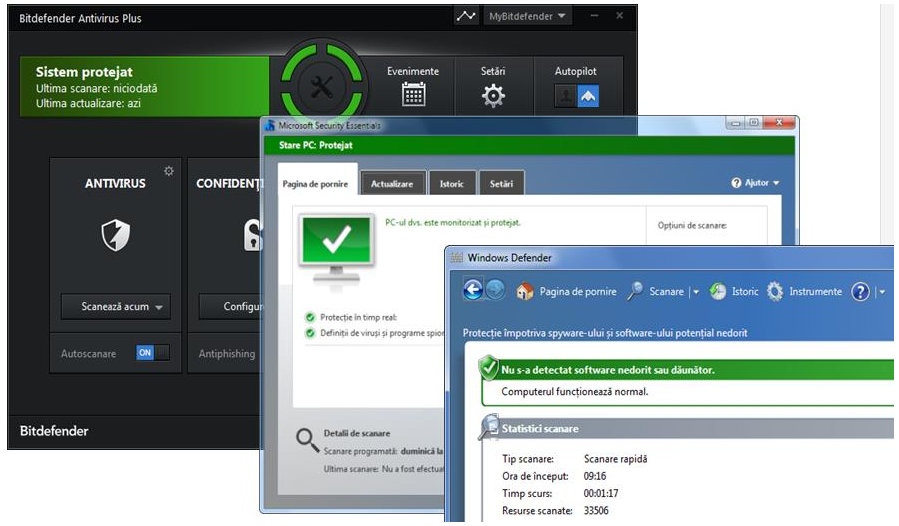
- **Reducerea Riscului de inginerie socială**
  - Cel mai eficient mod de a evita să devii victima ingineriei sociale este să cunoști cele mai răspândite practici de inginerie socială
    - Poziționarea ca tehnician și utilizarea autorității ce implică această funcție pentru a-i determina pe angajați să divulge informații, să modifice configurările serverelor sau să obțină informații sensibile
    - Derutarea sau intimidarea unui angajat ori a paznicului ca să permită accesul fizic în clădire
    - Expedierea mesajelor prin email cu aspect oficial tuturor angajaților conținând instrucțiuni care îi determină să dezvăluie informații sensibile

Identificarea Riscurilor

- **Phishing-ul**
  - *Phishing-ul* este procesul prin care se încearcă colectarea de informații sensibile
  - De regulă, un piser expediază un mesaj prin email cu aspect oficial care pare să fi venit de la o sursă legitimă
    - Mesajul din email, în general, conține o alertă falsă și instrucțiuni de a acționa într-un anumit mod
  - Ca să te protejezi de phishing:
    - Activează caracteristicile anti-phishing din browserele tale
    - Verifică manual site-urile necunoscute
    - Evită să urmezi link-urile din mesajele de email
    - Înainte să te conectezi pe un site sigur, verifică bara de Adresă ca să te asiguri că adresa începe cu numele legitim al site-ului

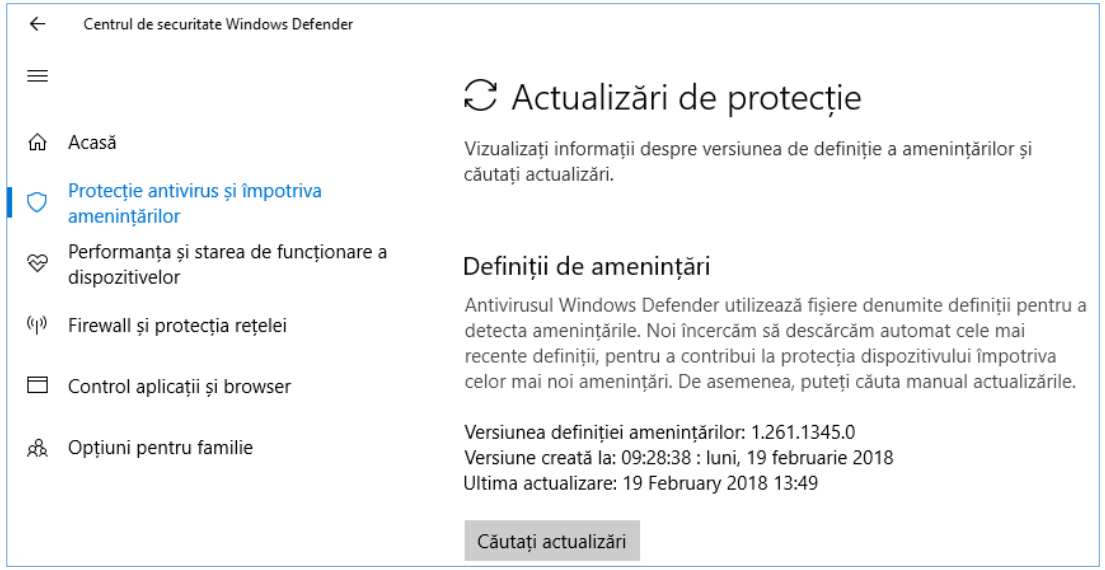
Cum să te protejezi

- **Software de antivirus**
  - Utilizează software de antivirus pentru a scana computerul tău de viruși cunoscuți și pentru a elimina orice virus depistat
  - Majoritatea programelor de antivirus conțin componente de anti-spyware
  - Poți demara în mod manual scanarea sistemului tău sau poți planifica scanări periodice utilizând setările programului



Cum să te protejezi

- Imediat ce ai instalat software-ul de antivirus, scanează computerul pentru a identifica orice viruși posibili care s-ar putea deja să existe în sistem
- Se recomandă să programezi scanări periodice ale sistemului
- În plus, abonează-te imediat la actualizări automate ale fișierelor de definire a virușilor
- Toate versiunile de software de antivirus includ actualizări frecvente și gratuite ale fișierelor de definire a virușilor, care permit programului să recunoască și să elimine cei mai recenți viruși



Cum să te protejezi

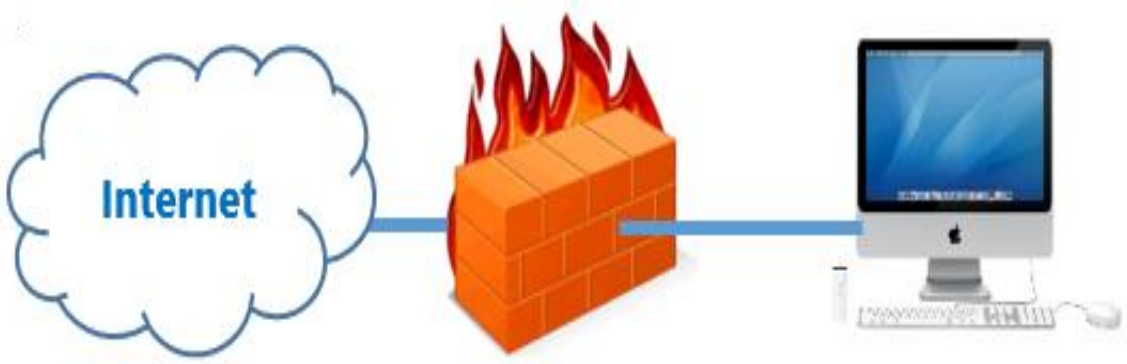
- **Evitarea virușilor**
  - Salvând și apoi scanând toate fișierele pe care le descarci din Internet (înainte să le rulezi sau să le deschizi)
  - Scanând discurile amovibile înainte să copiezi sau să deschizi fișierele care se conțin pe acestea
  - Dacă partajezi fișiere cu alte persoane utilizând dispozitive portabile, scanează toate fișierele pe care vrei să le partajezi, ca să te asiguri că nu le transmiți din neatenție un virus
  - Configurează-ti programul de antivirus astfel încât acesta să scaneze întotdeauna toate mesajele de email atât cele primite, cât și cele trimise
  - Scanează, de fiecare dată, fișierele atașate la email înainte de a le deschide
  - Fii prudent cu orice atașare neașteptată primită cu un email sau printr-o transmisiune de mesaj instant
    - Nu deschide atașarea
    - Încearcă să contactezi expeditorul mesajului (folosind o altă metodă decât prin email) și află dacă atașarea este legitimă
    - Dacă este imposibil să contactezi expeditorul sau acesta nu este la curent cu atașarea, șterge atașarea din mesaj
    - Deschide folderul tău cu articole șterse și șterge atașarea și de aici, pentru a o elimina definitiv din sistemul tău

Cum să te protejezi

- **Eliminarea virușilor**
  - Când un program de antivirus rulează, se vor scana fișierele pe care le-ai selectat; dacă identifică un virus sau o amenințare, programul îți va oferi opțiunea carantină sau elimină amenințarea
  - Dacă alegi să pui fișierele infectate în carantină, programul de antivirus le va plasa într-o zonă, de unde nu pot infecta alte fișiere
  - Dacă alegi să elimini fișierul, programul de antivirus îl va șterge definitiv din sistemul tău
  - În cazul în care programul de antivirus identifică un virus care nu poate fi eliminat, acesta, la fel, va plasa fișierul infectat în zona de carantină și va încerca să găsească un instrument de eliminare a respectivului virus pe pagina web a programului de antivirus
  - Este extrem de important să păstrezi software-ul de antivirus actualizat la zi și configurat să descarce în mod automat actualizări
  - Este la fel de important să menții activă opțiunea programului de scanare a emailului și cea de scanare rezidentă

Cum să te protejezi

- **Paravane de protecție**
  - *Paravanul de protecție* este o barieră de securitate care filtrează și controlează fluxul de informații care intră și iese dintr-o rețea privată
  - Filtrele folosite de paravanele de protecție sunt ansambluri de reguli simple care definesc și controlează tipurile de trafic care este permis și care trebuie blocat



Cum să te protejezi

- Într-o organizație, administratorul de rețea poate institui și implementa reguli de securitate aferente paravanului de protecție care să controleze modul în care angajații folosesc Internetul
- Paravanul de protecție protejează rețeaua ta de activitățile malițioase parvenite din exterior și oferă o "ușă" prin care persoanele pot comunica între rețeaua securizată(LAN) și Internet care este deschis și nesigur
- Paravanul de protecție poate fi un computer dedicat, un dispozitiv specializat – paravan de protecție sau poate fi implementat într-un dispozitiv de rețea
- Într-un mediu de rețea de domiciliu sau dintr-un mic oficiu, unde este folosit un router de bandă largă, paravanul de protecție este, de regulă, încorporat în routerul de bandă largă

Cum să te protejezi

- **Paravanele de protecție pentru Desktop**
  - Cunoscute ca paravane de protecție personale, paravanele de protecție pentru desktop oferă protecție unui sistem individual și nu întregii rețele
  - Paravanele de protecție pentru Desktop oferă multe caracteristici
  - Când paravanul de protecție este folosit împreună cu un program de antivirus, computerul personal este securizat, cu condiția că utilizatorul actualizează aceste aplicații frecvent
  - Multe sisteme de operare au incorporate software de paravan de protecție pentru desktop

Cum să te protejezi

- **Obstacole provocate de paravanele de protecție**
  - Paravanele de protecție pot prezenta obstacole utilizatorilor de rețea
  - Uneori, setările paravanului de protecție blochează accesul la anumite site-uri web sau blochează intrarea în rețea pentru redarea în flux a fișierelor audio ori video
  - De asemenea, poți descoperi că serviciul sau pagina web, pe care vrei să o accesezi, este în conflict cu politica de securitate din organizația ta

Cum să te protejezi

- **Software de monitorizare**
  - Majoritatea administratorilor de rețea protejează rețeaua cu ajutorul software-ului de monitorizare pentru a urmări și înregistra activitatea din rețea
  - În unele organizații, administratorii duc monitorizarea la cu totul alt nivel, instalând software de supraveghere a PC pentru a înregistra toate activitățile desfășurate, permițând-i administratorului să capteze intrările de la tastatură, să vizualizeze capturi de ecran și să vadă conversațiile tale din email, mesageria instantă și activitatea ta din web
  - Ține minte, computerele din școală sau de la locul de muncă nu sunt proprietatea ta privată

Cum să te protejezi

- **Efectuarea sigură a tranzacțiilor de E-Comerț**
  - Nivelul tău de siguranță în efectuarea tranzacțiilor determină volumul de e-comerț și de cumpărături online pe care le faci
  - **Fii Selectiv**
    - Dacă vrei să efectuezi achiziții în online, efectuează-le de la companiile cu reputație bună și despre care se cunoaște că oferă:
      - Servicii bune pentru clienți
      - Livrare de încredere
      - Politică de returnare echitabilă și facilă
    - Alege cu atenție site-urile de comerț electronic
    - Site-urile legitime de e-comerț afișează pe pagina lor web link-uri către political lor privată și către regulile referitoare la termene și condiții

Cum să te protejezi

- **Exersează Scepticismul**
  - Dacă o companie oferă o tranzacție care pare să fie prea bună pentru a fi adevărată, reverifică oferta
  - Ia aceleași măsuri de precauție pe care le-ai lua dacă cineva ti-ar face aceeași ofertă offline
  - Dacă nu îți este cunoscută compania, fă o cercetare despre aceasta înainte să cumperi ceva online
  - Apelează numerele de contact afișate pe site, caută lista de clienți sau a referințelor/comentariilor clienților și caută informații despre aceste companii cu ajutorul organizațiilor care urmăresc comentariile bune sau rele despre companii

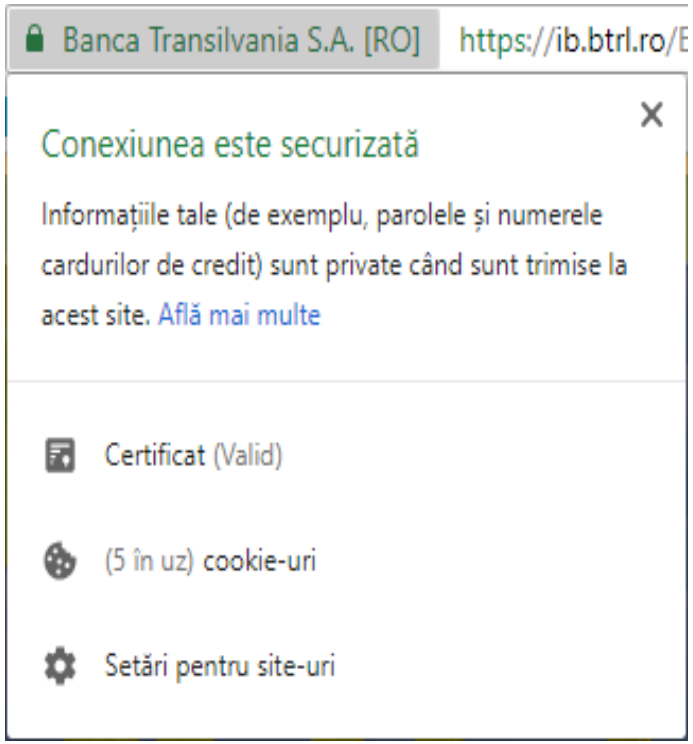
Cum să te protejezi

- **Folosește întotdeauna tranzacții securizate**
  - Cât navighezi pe Internet, browser-ul tău utilizează *protocolul de transfer hypertext* („**h**yper**t**ext **t**ransfer **p**rotocol" - http)

  - Ca să poți efectua tranzacții sigure pe Internet, serverele web utilizează *protocolul hypertext de transfer sigur* pentru criptarea tuturor informațiilor trimise între computerul tău și serverul web („**h**yper**t**ext **t**ransfer **p**rotocol **s**ecure" - https)

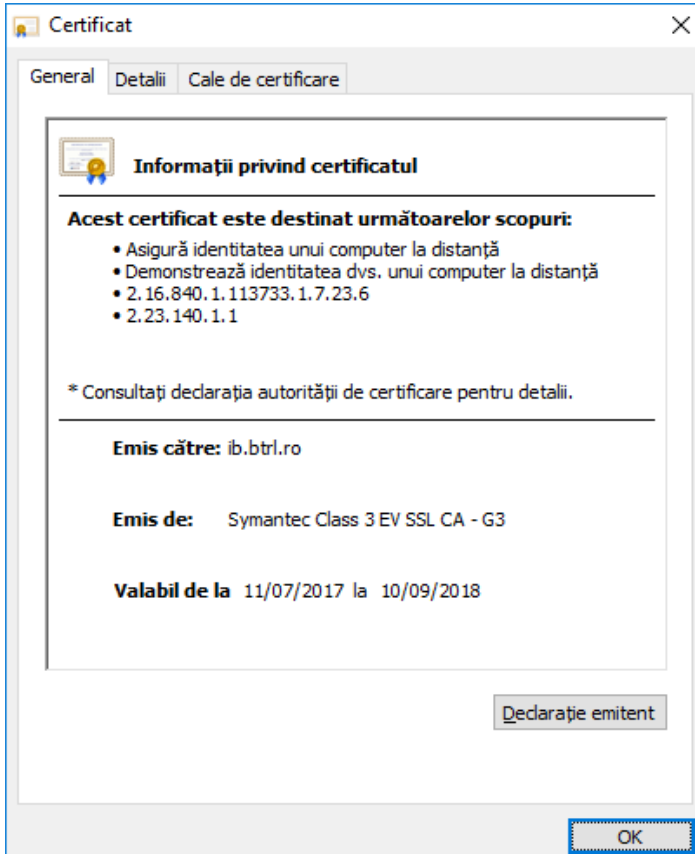
Cum să te protejezi

- Protocolul https și o pictogramă cu lacăt în bara de Adrese indică faptul că te afli în zona securizată a paginii web a vânzătorului și că tranzacția poate fi efectuată în siguranță
- Tranzacțiile web sunt securizate prin criptare, care este un proces de conversie a informației într-o formă care nu poate fi citită



Cum să te protejezi

- *Certificatul digital* este un fișier de mici dimensiuni care furnizează identitatea unei persoane sau a unei companii în Internet
- Autoritatea competentă, denumită *Autoritatea de Certificare* (CA), este responsabilă să verifice legalitatea certificatelor digitale
- Întotdeauna, caută protocolul https și pictograma lacăt ca să te asiguri că efectuezi tranzacții sigure în Internet
- Browser-ul tău are incorporate caracteristici care îți permit să știi când tranzacțiile sunt sigure



Cum să te protejezi

- **Rețele Virtuale Private („Virtual Private Networks” - VPNs)**
  - Conectarea din exteriorul rețelei este cunoscută ca acces la distanta
  - Securitatea este o component deosebit de importantă a accesului la distanta deoarece comunicarea prin rețeaua publică este vulnerabilă din punctul de vedere al posibilelor interceptări
  - *Autentificarea* este procesul de confirmare a identității unui utilizator sau a unui computer
  - *Criptarea* este procesul de conversie a informației în text indescifrabil, care necesită o cheie de decriptare pentru a putea fi citită
  - O VPN este o conexiune criptată între două computere, care asigură comunicarea securizată, privată la mare distanta utilizând Internetul ca platformă de comunicare, în locul unei linii private dedicate
  - VPN-urile dau posibilitatea angajaților care se află în deplasare de serviciu sau celor care lucrează de la distanta, sau locațiilor satelit să stabilească conexiune securizată cu rețeaua companiei din exteriorul sediilor acesteia

Cum să te protejezi

- **Utilizarea VPN-urilor**
  - Angajații care lucrează de la distanta sau cei care se află în deplasare de serviciu folosesc VPN pentru a se conecta la rețelele companiei din exteriorul acestora
  - Pentru ca o rețea să ofere conexiune VPN, este necesar ca serverul VPN să fie configurat să primească conexiuni de intrare
  - Orice utilizator care dorește să creeze o conexiune VPN dintr-o locație aflată la distanta trebuie să instaleze și apoi să lanseze programul client VPN pentru a deschide conexiunea cu serverul VPN
  - Utilizatorii trebuie să se conecteze folosind un nume și parolă de utilizator valide, exact ca și când s-ar conecta la rețea din interiorul oficiului

Copierea de rezervă și Restaurare

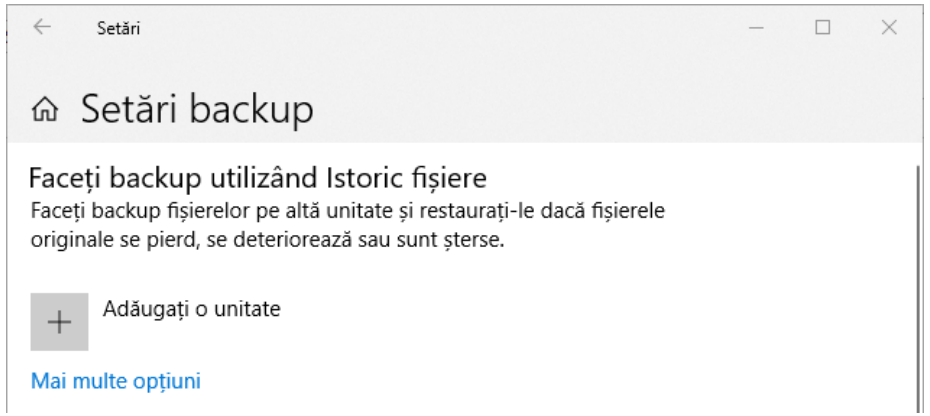
- *Backup-ul* este o copie a unui program, unui disc sau informației, realizat fie în scop de arhivare fie pentru a proteja fișierele de pierdere în cazul în care originalul s-ar deteriora sau distruge
- Backup-urile trebuie înscrise pe un mediu de stocare diferit de cel al sursei backup-ului
- Dispunerea de backup curent pentru cele mai importante fișiere este esențială pentru asigurarea faptului că informația ta poate fi recuperată în eventualitatea distrugerii sau pierderii acesteia
- Windows conține caracteristici încorporate care fac comod și facil atât backup-ul informației de sistem, cât și al fișierelor personale

Copierea de rezervă și Restaurare

- **Copierea fișierelor pe un spațiu de stocare cloud** – se face la fel de ușor ca și cum ai glisa fișierele importante în folderul tău local OneDrive, Drive, Dropbox sau iCloud
- **Folosirea Istoric Fișiere în Windows 10** – această caracteristică configurează Windows 10 să creeze în mod automat, în fiecare oră, backup-ul fișierelor tale personale, când mediul de destinație este conectat la PC
- **Utilizarea utilitarului Windows Copiere de rezervă și Restaurare** – Acesta este un utilitar inclus în Windows 7 care configurează Windows să creeze în mod automat, săptămânal, copii de rezervă pentru toate fișierele importante din computer; acestea includ fișierele tale personale și fișierele salvate în folderele implicite Windows utilizate de sistemul de operare

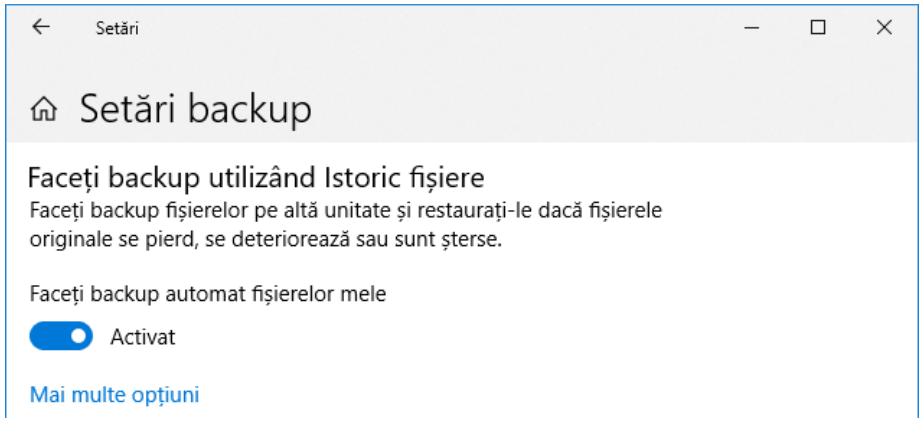
Copierea de rezervă și Restaurare

- **Istoric fișiere**
  - Pentru a configura utilitarul, conectează o unitate de disc externă, deschide aplicația **Setări**, fa clic pe **Actualizare și securitate**, apoi, în panoul din stânga al ferestrei, apasă **Setări backup**



Copierea de rezervă și Restaurare

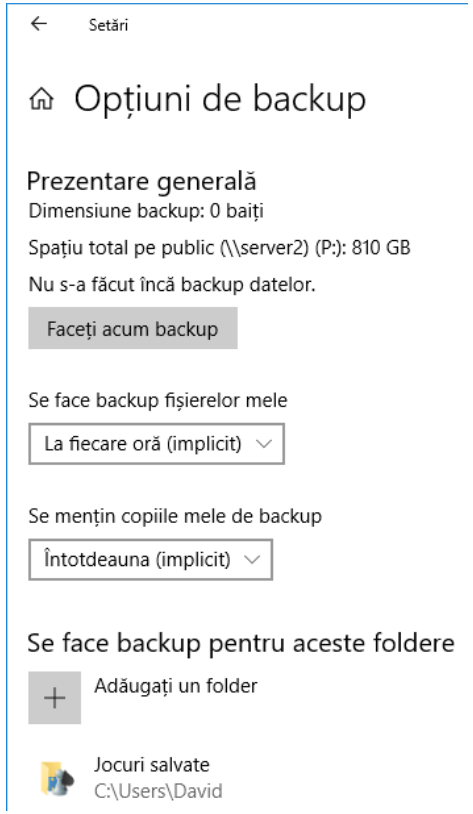
- Fă clic pe **Adăugați o unitate**, apoi selectează Unitate externă în fereastra *Selectați o unitate* pentru a afișa Copiere de rezervă automata pentru fișierele mele



- Accesează **Mai multe opțiuni** pentru a vizualiza pagina Opțiuni copiere de rezervă

Copierea de rezervă și Restaurare

- Folosește setările de pe această pagină pentru a gestiona frecvența realizării copiilor de rezervă și durata păstrării fișierelor copiilor de rezervă
- Poți crea o copie de rezervă imediat accesând butonul **Faceți acum backup**, și poți specifica care foldere din profilul tău de utilizator să fie incluse în backup
- În mod implicit, aceste foldere sunt: Desktop, Documente, Descărcări, Muzică, Imagini, Videoclipuri și altele
- La necesitate, poți adăuga sau exclude foldere

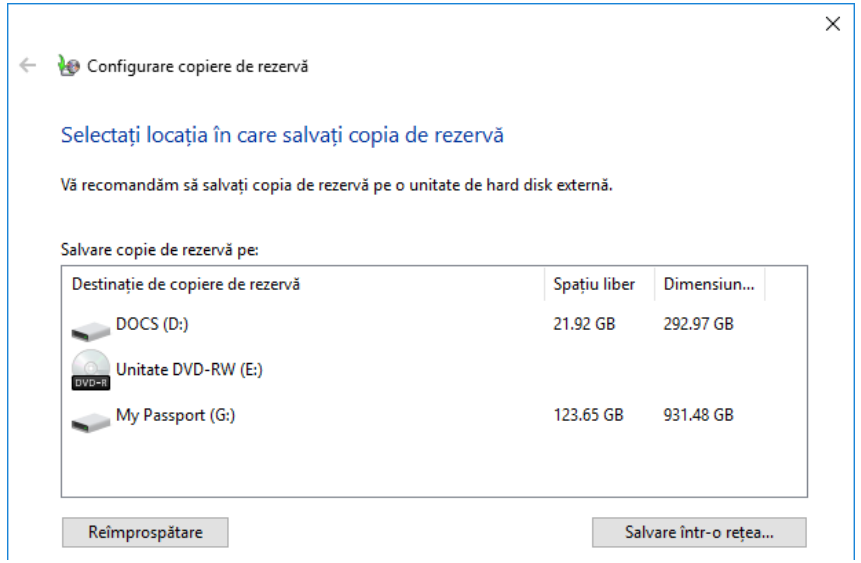


Copierea de rezervă și Restaurare

- **Copiere de rezervă și Restaurare în Windows**
  - Poți folosi utilitarul Copiere de rezervă și Restaurare din Windows pentru a face backup-ul întregului sistem sau doar a anumitor fișiere și foldere pe care le selectezi
  - Poți alege să-i permiți Windows să selecteze elementele pentru backup sau poți selecta foldere individuale, biblioteci și unități pentru care vrei să faci backup
  - În mod implicit, backup-urile sunt create periodic, conform unui plan, pe care îl poți modifica sau poți oricând crea o sesiune de backup în mod manual
  - Din moment ce ai configurat Windows Backup, Windows urmărește fișierele și folderele noi sau care au fost modificate și le adaugă la backup

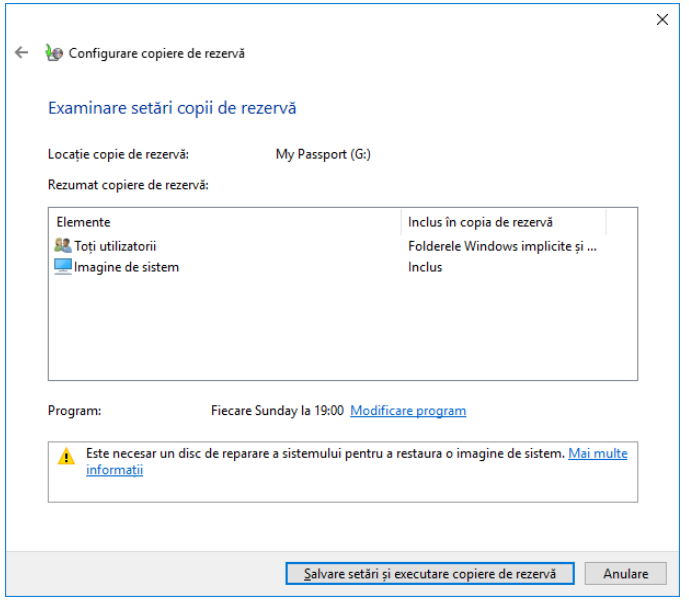
Copierea de rezervă și Restaurare

- Dacă nu ai mai folosit niciodată Windows Backup, vei fi nevoit, întâi, să-l creezi urmând pașii din wizard
- Deschide Panoul de Control și navighează la **Sistem și Securitate**, fă clic pe pagina **Backup și Restaurare (Windows 7)**, apoi apasă **Modificare setări**



Copierea de rezervă și Restaurare

- Selectează destinația pentru fișierele din backup, apoi apasă **Următorul**
  - În mod implicit, Windows va face backup pentru informațiile salvate în biblioteci, pe Desktop și din folderele implicite Windows
  - Windows, de asemenea, va crea o imagine de sistem, care poate fi folosită pentru restaurarea computerului, în cazul în care acesta încetează să funcționeze
- Apasă **Următorul** dacă accepți setările implicite sau fă clic pe **Se permite alegerea** pentru a specifica setări personalizate

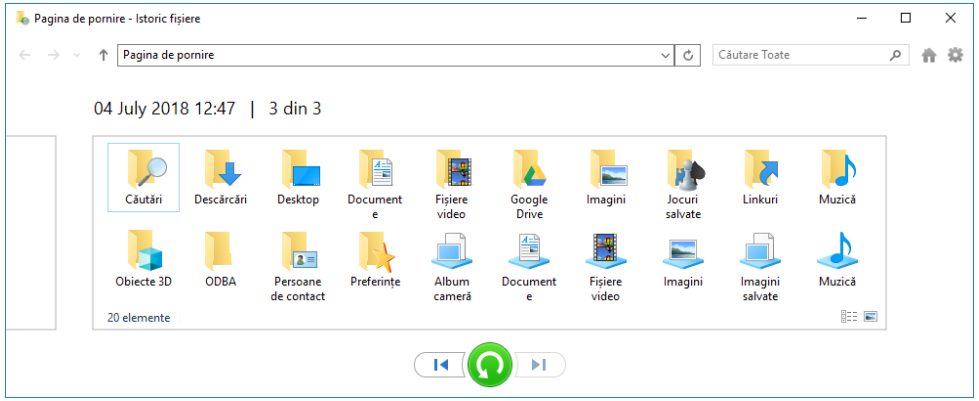


Copierea de rezervă și Restaurare

- Apasă **Modificare program** dacă dorești să ajustezi backup-ul programat
  - În mod implicit, Windows efectuează backup în fiecare zi de duminică la ora 19:00
  - Poți configura Windows să efectueze backup în fiecare zi, săptămână sau lună
  - Poți, de asemenea, să specifici că nu dorești să programezi backup-uri viitoare
- Fă clic pe **Salvare setări și executare copie de rezervă** pentru a efectua backup

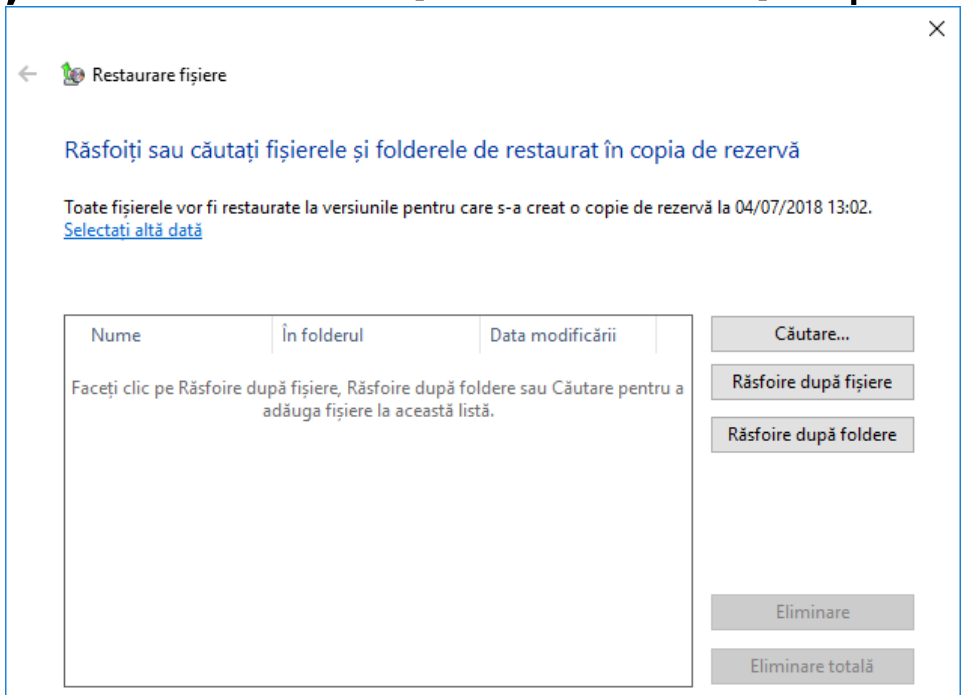
Copierea de rezervă și Restaurare

- **Restaurarea fișierelor personale**
  - Dacă ai șters, din întâmplare, un fișier sau dacă acesta este corupt, îl poți restaura cu ușurință pe unitatea ta de disc de pe suportul pe care s-a salvat backup-ul
  - Dacă ai făcut backup utilizând OneDrive, pur și simplu copiază fișierele sau folderele necesare din folderul OneDrive și lipește-le pe unitatea ta de disc utilizând File Explorer
  - În cazul în care ai făcut backup utilizând utilitarul Istoric Fișiere, deschide aplicația Setări, fă clic pe **Setări backup**, apoi **Mai multe opțiuni**, derulează la sfârșitul ferestrei și fă clic pe **Restaurarăți fișiere dintr-o copie backup curentă**



Copierea de rezervă și Restaurare

- În cazul în care ai efectuat backup utilizând Copiere de rezervă și Restaurare, deschide Panoul de Control și navighează la **Sistem și Securitate**, fă clic pe pagina **Backup și Restaurare (Windows 7)**, apoi pe butonul **Restaurați fișierele mele** pentru a deschide fereastra *Restaurare Fişiere*
- Folosește butoanele *Răsfoire după fișiere* și *Răsfoire după foldere* pentru a selecta fișierele și folderele pe care vrei să le restaurezi



Copierea de rezervă și Restaurare

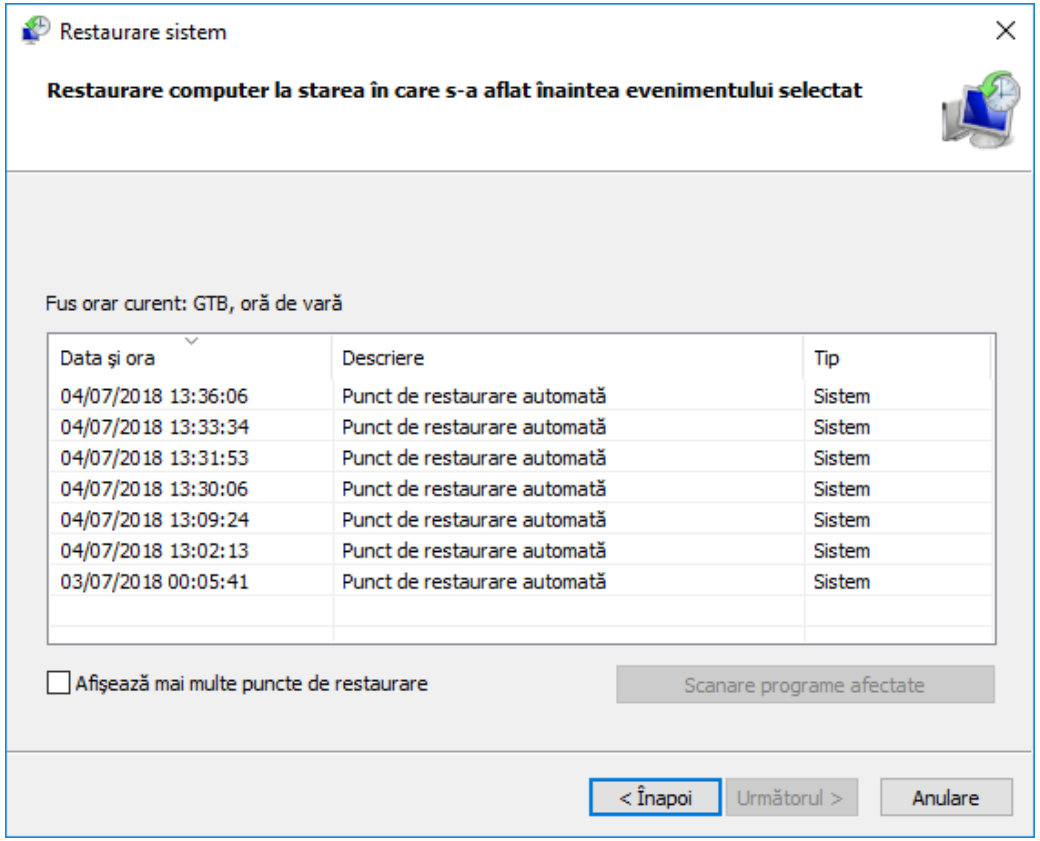
- **Copii de rezervă securizate**
  - Organizațiile, care operează cu informațiile personale ale altor oameni, sunt obligate prin lege să păstreze și să securizeze backup-uri pentru un anumit număr de ani
    - Backup-urile trebuie să fie redundante
    - Cel puțin o copie de backup trebuie să fie depozitată în afara sediului
    - Locațiile de depozitare din afara sediilor trebuie să fie securizate
    - Backup-urile trebuie să fie criptate
    - Backup-urile trebuie verificate

Copierea de rezervă și Restaurare

- **Copiere de rezervă a fișierelor și setărilor de sistem**
  - Fișierele de sistem sunt vitale pentru buna funcționare a sistemului de operare, iar, în timp, acestea pot deveni corupte
  - Windows are încorporate câteva instrumente pe care le poți folosi pentru a realiza backup-ul fișierelor de sistem:
    - Puncte de restaurare a sistemului
    - Fișiere Imagini de sistem

Copierea de rezervă și Restaurare

- **Puncte de restaurare a sistemului**
  - Un *punct de restaurare* este o fotografie salvată a fișierelor sistemului tău Windows, a fișierelor de tip program și a setărilor Windows Registry, realizată la un moment dat



Copierea de rezervă și Restaurare

- Cum te asiguri că această comandă de protecție este activată în sistemul tău Windows 10:
  1. Faci clic în caseta de căutare din bara de activități, apoi scrii: **punct**
  2. Faci clic pe **Creare punct de restaurare** în meniul Start pentru a deschide fila *Protecție sistem* din caseta de dialog *Proprietăți sistem*
  3. Faci clic pe unitatea ta de disc din caseta tip listă cu unitățile disponibile. Dacă se afișează *Activată* în coloana *Protecție*, comanda este activată
  4. Dacă protecția unității de disc este inactivă, fă clic pe **Configurare**
  5. Apasă **Activare protecție sistem**
  6. Glisează indicatorul pentru **Utilizare maximă** la aproximativ 5% (între primele două marcaje de bifare din scara de gradație). Aceasta va aloca o porțiune din unitatea de disc pentru stocarea punctelor de restaurare
  7. Fă clic pe **Se aplică**, apoi **OK**
  8. Mai apasă o dată **OK** pentru a închide caseta de dialog Proprietăți sistem

Copierea de rezervă și Restaurare

- Când este activată, comanda Restaurare Sistem creează, în mod automat, puncte de restaurare o dată pe săptămână, și înainte de evenimentele majore de sistem
- Cum creezi, în mod manual, puncte de restaurare:
  1. Faci clic în caseta de căutare din bara de activități, apoi scrii: **restaurare**
  2. Faci clic pe **Creare puncte de restaurare** în meniul Start pentru a deschide fila *Protecție sistem* din caseta de dialog *Proprietăți sistem*
  3. Apasă **Creare...**
  4. Scrie un nume pentru punctul de restaurare, apoi fă clic pe **Creare**
  5. Când apare mesajul că punctul de restaurare a fost creat cu succes, fă clic pe **Închidere** apoi pe **OK**.

Copierea de rezervă și Restaurare

- Când efectuezi o restaurare dintr-un punct de restaurare, comanda Restaurare Sistem restaurează fișierele de sistem, fișierele program și setările de Registry
- S-ar putea să ai nevoie de un specialist tehnic care să te ghideze cum să întorci sistemul tău la un punct de restaurare:
    1. Faci clic în caseta de căutare din bara de activități, apoi scrii **Restaurare**
    2. Faci clic pe **Creare puncte de restaurare** în meniul Start pentru a deschide fila *Protecție sistem* din caseta de dialog *Proprietăți sistem*
    3. Faci clic pe **Restaurare sistem...**, apoi pe **Următorul** pentru a afișa lista punctelor de restaurare salvate. La începutul listei se afișează cele mai recent create puncte de restaurare. Pentru a vizualiza puncte de restaurare mai vechi, poți selecta din caseta de bifare apăsând **Afișează mai multe puncte de restaurare**
    4. Selectează punctul de restaurare la care vrei să întorci sistemul, apoi apasă **Următorul**
    5. Faci clic pe **Terminare** și urmezi instrucțiunile care apar.

Copierea de rezervă și Restaurare

- **Imagine de Sistem / Repararea unității**
  - *Imaginea de sistem* este imaginea exacta a unității de disc. Aceasta conține setările Windows și ale sistemului tău, programe și fișiere
  - Poți crea o imagine de System oricând, urmând acești pași:
    1. Conectează o unitate de disc externă sau alt suport amovibil cu capacitate mare de stocare.
    2. Fă clic pe **Backup și Restaurare (Windows 7)** din Panoul de control
    3. Fă clic pe link-ul **Creare imagine de sistem**
    4. Selectează suportul pe care să se creeze imaginea, apoi apasă **Următorul**
    5. Confirmă setările, apoi apasă **Pornire copiere de rezervă**
    6. Un specialist tehnic te poate ghida în procesul de restaurare a sistemului tău de pe un fișier imagine sau poți furniza suportul conținând respectivul fișier imagine unui specialist dacă acesta se va ocupa de reparație.

Copierea de rezervă și Restaurare

- **Copii de rezervă ale informațiilor de pe dispozitivele portabile**
  - Este întotdeauna foarte util să faci copii de rezervă a informațiilor de pe dispozitivele tale portabile.
  - Utilizează un cablu USB pentru a copia informațiile pe PC-ul tău, sau folosește utilitățile de backup încorporate în telefonul tău și serviciul de stocare în Cloud asociat
  - **Android**
    1. Deplasează-te la **Setări, Personale, Backup și resetare**
    2. Activează ambele opțiuni: **Back up informațiile mele** și **Restaurare Automată**
    3. Contul de backup trebuie să fie setat pe contul de Gmail

Copierea de rezervă și Restaurare

- **iPhone/iOS**
  - Cum faci backup utilizând iCloud:
    1. Conectează dispozitivul la o rețea Wi-Fi
    2. Deschide **Configurări**, **iCloud**, **Backup**
    3. Asigură-te că iCloud Backup este activat
    4. Atinge **Back Up acum**
    5. Cum faci backup utilizând iTunes:
    6. Deschide iTunes și conectează dispozitivul tău la computer.
    7. Salvează conținutul descărcat din iTunes Store sau din App Store făcând clic pe **Fișier, Dispozitive, Transferare Achiziții**
    8. Pentru a crea un backup, apasă **Back Up acum**

Copierea de rezervă și Restaurare

- **Utilizarea opțiunilor de resetare de fabrică a unui PC**
  - Când folosești opțiunea Resetare de fabrică din dispozitivul tău, de fapt, resetezi dispozitivul la configurările pe care le avea în momentul în care a ieșit din fabrică
  - **Înainte să resetezi dispozitivul, întotdeauna** creează un backup pentru fișierele tale personale
  - **Reîmprospătarea și Resetarea Windows 10**
    - **Reîmprospătarea PC-ului** presupune o nouă instalare a Windows fără ca fișierele tale personale, setările tale personalizate sau aplicațiile pe care le-ai instalat din Windows stare, să fie șterse.
    - **Resetarea PC-ului** presupune o nouă instalare de Windows care nu păstrează nici un element. Este ca o formatare a unității de disc și presupune reinițierea lucrului cu o nouă instalare a sistemului de operare.
    - Cum faci Reîmprospătarea sau Resetarea PC-ului Windows 10:
      1. Apasă **Start**, **Setări**, **Actualizare și securitate**
      2. Fă clic pe **Recuperare**, apoi sub Resetare acest PC, apasă Începeți.
      3. În caseta pentru A*legeți o opțiune*, selectează fie *Păstrați fișierele mele* sau *Eliminați tot*

Copierea de rezervă și Restaurare

- **Resetarea dispozitivelor portabile**
  - Dispozitivele portabile conțin comanda Resetare de fabrică, care restaurează dispozitivul la configurările pe care le avea în momentul ieșirii din fabrică.
  - Resetarea telefonului sau a tabletei tale poate fi necesară în scopul depanării.
  - Tine minte, dacă folosești un dispozitiv GSM, cardul SIM instalat conține informațiile contului tău personal.
  - **Scoate, de fiecare data, cardul tău** SIM înainte să dăruiești sau să transmiți telefonul tău altei persoane.
  - **Înainte de a reseta, se recomandă să faci, de fiecare dată,** backup-ul fișierelor tale personale.

Copierea de rezervă și Restaurare

- **Android**
  - Poți observa că, suplimentar opțiunii de Resetare de fabrică, există opțiunea resetare doar a configurărilor telefonului sau de resetare a configurărilor de rețea.
  - Cum restaurezi dispozitivul tău Android la configurările de fabrică:
    1. Mergi la **Setări**, **Personale**, **Backup și resetare**
    2. Atinge Resetare de fabrică
    3. Atinge **Resetare telefon**
  - Dacă telefonul sau tableta au memorie expandabilă, meniul te poate întreba dacă dorești să ștergi cardul de memorie externă, ceea ce nu este neapărat necesar, deoarece poți scoate cardul din slut

Copierea de rezervă și Restaurare

- **iPhone/iOS**
  - În versiunile de iOS 7 și mai mult, există o caracteristică de securitate denumită Blocarea activității, care solicită ID-ul Apple utilizat pentru a configura telefonul la setările de bază.
  - Cum deconectezi iCloud/Găsire iPhone:
    1. Deschide Configurări
    2. Atinge **iCloud**
    3. Derulează în josul ecranului și atinge Ieșire. Introdu ID-ul și parola ta Apple /iCloud dacă ti se cere
  - Cum restaurezi dispozitivul tău iOS la configurările de fabrică:
    1. Deschide Configurări
    2. Atinge **General**
    3. Atinge **Resetare**
    4. Atinge Ștergeți conținut și configurări și introdu codul de acces dacă ti se solicită
    5. Atinge **Șterge** pentru a începe

Depanarea

- *Depanarea* este abordarea sistematică de soluționare a problemelor.
- Este posibil să fie nevoie să încerci mai multe și diferite abordări până să identifici o soluție, de regulă, însă, se folosește procesul de eliminare
- Mai jos sunt câteva sfaturi generale pentru depanare:
  - Notează pașii, aceasta te va ajuta să memorizezi ce ai făcut deja și să eviți testarea repetată a acelorași cauze posibile
  - Fă notițe detaliate a mesajelor de erori pe care le vezi, scrie cât mai multe informații sau utilizează instrumentul de decupare încorporat în Windows pentru a face capturi de ecran conținând mesajele de eroare

Depanarea

- **Este o problemă de hardware sau de software?**
  - **Hardware**
    - Hardware-ul pe care îl vei depana adesea este mare și autonom.
    - Când investighezi problemele posibile de hardware, începe cu cele mai evidente:
      - Este dispozitivul conectat la sursa de curent electric?
      - Conexiunea este bună?
    - Există probleme ușor detectabile aferente dispozitivului de hardware, care necesită a fi rezolvate ca dispozitivul să poată funcționa?

Depanarea

- **Software**
  - Ai instalat recent actualizări?
  - Dacă închizi și repornești programul, problema persistă?
  - Repornirea computerului și apoi relansarea programului soluționează problema?
  - Este programul actualizat la zi? Poți găsi și instala actualizări pentru acesta?
  - Poți rula programul în modul de compatibilitate?
  - Dacă sistemul tău se blochează constant sau nu se lansează corect după ce a fost efectuată o actualizare, rularea înapoi a actualizării la un punct de restaurare va soluționa problema?
  - Este posibil ca sistemul tău să fie infectat cu un virus? Execută o scanare de viruși ca să te asiguri că nu există nici o infecție care să interfereze cu programele tale.

Depanarea

- **Depanarea problemelor de conectare**
  - Verifică adresa ta IP utilizând fie instrumentul Linia de comandă ipconfig sau Centrul de Rețea și Partajare din Windows.
  - Dacă adresa ta IP începe cu 169.254, sau dacă adresa ta IP se afișează ca 0.0.0.0, înseamnă că sistemul tău nu a primit o adresă IP validă de la router-ul de bandă largă din rețeaua ta de domiciliu.
  - În cazul în care sistemul tău nu a primit o adresă IP validă, încearcă să deconectezi router-ul de bandă largă pentru 20 de secunde, apoi repornește-l; ulterior repornește computerul.
  - Dacă sistemul tău are o adresă IP validă, dar nu te poți conecta la Internet, s-ar putea să fie necesar să repornești modemul tău de bandă largă.

Depanarea

- Dacă repornirea echipamentelor tale de rețea nu soluționează problema, apelează furnizorul tău de servicii de Internet.
- Când apelezi furnizorul de servicii de Internet, fii gata să oferi informații precum ar fi adresa ta curentă IP și viteza ta de conectare.
- Dacă ai conexiune defectuoasă la rețeaua ta Wi-Fi, verifică următoarele:
  - Este activat adaptorul tău wireless?
  - A fost modificată parola de rețea Wi-Fi?
  - Ești suficient de aproape de hotspot ul Wi-Fi?
- Nu fii descurajat dacă depanarea durează ceva timp

Sumarul lecției

- explică nevoia de securitate
- descrie cum să păstrezi în siguranță numele tău de utilizator și parola
- descrie riscurile prezentate de viruși, viermi, Trojan și malware
- descrie riscurile asociate conexiunilor la rețea
- protejarea informației personale când utilizezi computere publice
- descrie riscurile prezentate de ingineria socială și atacurile de tip phishing
- descrie metodele de protecție împotriva producerii riscurilor
- explică cum și de ce se face back op și restaurarea informațiilor și a setărilor
- explică cum resetăm dispozitivele personale la setările lor de fabrică
- descrie tehnicile de bază de depanare

Întrebări recapitulative

1. Care dintre următoarele parole este cea mai sigură?
   a. NeXt-Chg9917A
   b. PaSW0rd
   c. Nextchg9917
   d. pA$$word003
2. Cum accesezi comanda de blocare utilizând meniul Start?
   a. Faci clic pe butonul Start, pe denumirea contului tău de utilizator apoi pe Blocare.
   b. Faci clic pe Start, pe Închidere Windows, apoi pe Blocare.
   c. Faci clic pe Start, Închidere și apoi pe Blocare.
   d. Poți accesa comanda de Blocare doar din pagina Opțiuni de închidere din Panoul de control.

Întrebări recapitulative

3. Computerul lui Eduardo a început să afișeze mesaje ciudate de eroare, iar apoi tot ce a fost în folderul său Documente s-a șters. Probabil, Eduardo a devenit victima unui:
   a. Virus
   b. Configurare defectuoasă de sistem
   c. Aplicație spyware
   d. Exploatare de tip Phishing
4. Un hacker poate obține acces de la distanta la computerul tău cu ajutorul unui:
   a. Cal Trojan
   b. Vierme
   c. Virus
   d. Adware
5. Care aplicație descarcă în mod automat publicitate?
   a. Adware
   b. Spyware
   c. Paravanul de protecție Desktop
   d. Software de monitorizare

Întrebări recapitulative

6. Care dintre următoarele nu este periculos și poate fi folosit pentru stocarea numelui de utilizator și a parolei?

   a. Cookie
   b. Spyware
   c. Adware
   d. Trojan

7. Claudia se conectează la rețeaua Wi-Fi din aeroport. Cum se recomandă să identifice această rețea Wi-Fi în sistemul ei de operare?

   a. Ca o rețea publică
   b. Ca o rețea de lucru
   c. Ca o rețea de domiciliu
   d. Ca o rețea privată

Întrebări recapitulative

8. Când utilizezi computere publice, ce altceva trebuie să mai faci în afară de a te deconecta de la conturile tale online?
   a. Să curăți cache-urile și cookie-urile.
   b. Să repornești computerul.
   c. Să deconectezi sursa de energie a computerului.
   d. Să blochezi sistemul.
9. Ce este practica de înșelare a oamenilor pentru ca aceștia să ofere acces neautorizat într-o clădire sau la un computer?
   a. Inginerie Socială
   b. Hacking
   c. Spyware
   d. Phishing

Întrebări recapitulative

10. Care dintre următoarele software-uri poate fi folosit pentru eliminarea virușilor din computer?

    a. Software de antivirus
    b. Paravanul de protecție desktop
    c. Software de monitorizare a rețelei
    d. Paravanul de protecție hardware

11. Care dintre următoarele previne intrarea traficului de rețea potențial periculos în rețeaua LAN?

    a. Un paravan de protecție
    b. Software de antivirus
    c. Un cache de browser
    d. Un modem

Întrebări recapitulative

12. Care dintre următoarele este conceput să urmărească și să înregistreze activitățile din rețea?

    a. Software de monitorizare
    b. Paravanele de protecție
    c. Conturile de conectare
    d. Software pentru Backup

13. Care dintre următoarele este conceput să urmărească și să înregistreze activitățile din rețea?

    a. HTTPS
    b. HTTP
    c. FTP
    d. SMTP

Întrebări recapitulative

14. Katarina este într-o călătorie și urmează să se conecteze în mod securizat la rețeaua companiei pentru a transmite câteva documente cu informații sensibile. Cum trebuie să realizeze această conexiune?

    a. Utilizând o VPN
    b. Utilizând un hot spot Wi-Fi
    c. Utilizând browserul ei web
    d. Utilizând browserul ei web și scrierea https ca protocol

15. Lee vrea să creeze o copie de rezervă a folderului său Documente. Care dintre următoarele locații este potrivită pentru stocarea backupului?

    a. O unitate de disc externă
    a. Pe Desktop
    c. Pe Desktopul altui profil de utilizator înregistrat pe computer
    d. Oricare dintre acestea este o locație potrivită pentru stocarea backupului

Întrebări recapitulative

16. În Windows 10 poți alege să faci backup-ul fișierelor personale copiindu-le în memoria cloud, sau utilizând Istoric Fișiere. Care este cea de a treia metodă?
    a. Utilizarea Copiere de rezervă și Restaurare din Windows
    b. Crearea unui punct de restaurare
    c. Utilizarea comenzii Reîmprospătarea acestui PC.
    d. Utilizarea comenzii Resetarea acestui PC.
17. Când creezi un punct de restaurare a sistemului, care fișiere nu se includ?
    a. Fișierele utilizatorilor
    b. Fișierele program
    c. Setările Registry
    d. Fișierele sistemului de operare

Întrebări recapitulative

18. Care dintre următoarele opțiuni poate fi folosită pentru a face backup-ul unui iPhone?

    a. iCloud
    b. Dropbox
    c. Google Drive
    d. OneDrive

19. Dacă computerul tău tinde să se închidă când lansezi o aplicație, ce tip de probleme s-ar putea că necesită a fi depanate?

    a. O problemă de software
    a. O problemă de hardware
    c. O problem legată de conexiunea la rețea
    d. O problemă legată de un nume invalid de utilizator

Întrebări recapitulative

20. Ann a folosit aceeași rețea Wi-Fi pe parcursul întregii zile. Și-a luat o pauză pentru a înota. Seara, însă, nu se poate conecta. Care dintre următoarele articole ar trebui verificate ca posibile cauze?
    a. Cardul ei wireless s-ar putea că nu mai este conectat.
    b. Router-ul wireless nu mai suportă standardul de wireless pe care ea îl folosește.
    c. Ea a introdus un nume de utilizator și parole greșite când s-a conectat la sistem.
    d. Rețeaua WLAN a devenit nesecurizată și nu îi permite să se conecteze.