Ghid de pregătire pentru certificarea IC3

Global Standard 4

Lecția 15: Cetățenie digitală

Obiectivele lecției

- Standardele pentru comunicarea profesională
- Cum să evitați comportamentul inadecvat în mediul online
- Proprietatea intelectuală, dreptul de autor și licențierea
- Noțiuni de ergonomie și amenajarea spațiului de lucru
- Protejarea computerului împotriva amenințărilor software
- Ce sunt virușii și cum să evitați infectarea computerului
- Protejarea activităților de comerț electronic

Probleme etice

- Pe măsură ce devine tot mai ușor să contribuim cu informații pe internet, sentimentul de anonimat poate să determine anumiți utilizatori să întreprindă anumite acțiuni în mediul online pe care nu le-ar întreprinde în mediul offline, sau să ignore drepturile de autor ori chestiuni legate de intimitate.
- Iluzia anonimatului în mediul online nu îi absolvă pe utilizatori de responsabilitate pentru comportamentul lor.
- Protejați-vă și păstrați același grad de respect și de bun simț în mediul online, pe care l-ați exercita în cadrul unei comunicări față în față.

Probleme etice

- **Proprietate intelectuală, drepturi de autor și licențe**
  - Informațiile de pe internet sunt disponibile gratuit pentru oricine dorește să le asculte, citească sau să le folosească în scop de divertisment.
  - Oamenii creează site-uri web din diverse motive
  - Doar pentru că informația se găsește pe un site web pe care îl puteți accesa liber, nu înseamnă că informația poate fi și copiată în mod gratuit, utilizată, distribuită sau prezentată ca și cum v-ar aparține.

Probleme etice

- **Proprietatea intelectuală**
  - Orice lucru creat sau inventat este „proprietatea intelectuală” a autorului.
    - Dacă a fost creat de o persoană sau de un grup în nume propriu.
    - Dacă a fost creat de o persoană sau de un grup, sub contract cu o organizație care a plăti valoarea serviciului, aparține acelei organizații”.
  - Estimarea adevăratei valori a proprietății intelectuale nu este o sarcină ușoară. Este foarte dificil să calculăm gradul pierderile pe care suferă persoana sau organizația a cărei proprietate a fost furată.
    - „Împrumutarea” proprietății intelectuale a cuiva poate însemna un lucru minor dar în realitate poate fi considerat furt, piratare sau chiar spionaj industrial.

Probleme etice

- **Drepturile de autor (*copyright*)**
  - Legile dreptului de autor au fost create pentru a proteja proprietatea
  - intelectuală.
  - Această lege se referă la protejarea oricărui material, publicat sau nepublicat, creat de o persoană sau de o organizație.
    - Este o lege care vă garantează dreptul asupra proprietății dvs. intelectuale.
    - Nimeni nu poate copia pictura pe care ați realizat-o, nu poate folosi codul site-ului web pe care l-ați creat și nu poate interpreta în public o piesă compusă de dvs. decât dacă-i dați acordul explicit.
  - Dreptul de autor conferă dreptul exclusiv de a vă vinde produsul.
    - Garantează că doar dvs. aveți dreptul de a vinde, împrumuta sau folosi în orice alt mod produsul dvs. în schimbul unei compensații.

Probleme etice

- **Înregistrarea dreptului de autor**
  - De îndată ce un produs original este pus într-o formă materială, produsul este protejat de dreptul de autor.
    - Protecția conferită de dreptul de autor începe în momentul finalizării produsului, până la 50 de ani după decesul autorului.
  - Produsele originale este indicat să aibă o notificare de copyright.
    - Anunțul va include simbolul dreptului de autor © (*Copyright*), urmat de data realizării și de numele autorului.
    - Este suficient pentru a emite anumite cerințe în cazul violării acestui drept.
  - Pentru a putea pretinde despăgubiri materiale trebuie însă să vă înregistrați produsul la OSIM (Oficiul de Stat pentru Invenții și Mărci).

Probleme etice

- **Materialele cu copyright de pe site-urile web**
  - Materialele prezentate pe un site web se supun acelorași reguli de copyright ca și informațiile publicate pe alte tipuri de medii.
  - Puteți folosi un material cu copyright numai dacă autorul vă dă dreptul.
    - Aceasta poate presupune plata unor taxe sau menționarea autorului atunci când utilizați respectivul material în produsul dumneavoastră.
    - Este responsabilitatea dvs. să determinați care sunt cerințele legate de copyright înainte de a folosi oricare parte a unui produs original.
  - *Fair Use* înseamnă că puteți folosi părți ale informației protejate prin drept de autor în scopul criticii sau al comentariilor fără a cere permisiunea celui care deține drepturile asupra acesteia.

Probleme etice

- Dreptul de autor aparține implicit deținătorului site-ului web sau al materialului publicat, chiar dacă simbolul dreptului de autor (©) și/sau textul nu apar pe produs.
  - Realizatorul poate să aibă patentul asupra produsului sau a tehnologiei, asta însemnând că acea persoană are drepturi exclusive să realizeze, să utilizeze și să vândă acel produs sau acea tehnologie.
  - Autorul poate alege să vă acorde o licență sau anumite drepturi de utilizare, dar nu puteți promova produsul sau tehnologia ca și cum v-ar aparține.
- Unele site-uri web vă permit să utilizați conținutul lor cu condiția de a-l cita corespunzător și de a specifica cine este autorul originar.
  - Fiți prudenți în astfel de cazuri pentru că proprietarul site-ului web, s-ar putea să nu fie creatorul originar al informației în cauză și de aceea nu are dreptul legal de a vă acorda astfel de permisiuni.

Probleme etice

- **Consecințe legale ale încălcării dreptului de autor**
  - Veți primi un document din partea autorităților, cerându-vă să eliminați conținutul de pe site-ul dvs. web, sau să ștergeți orice fișier descărcat.
  - Furnizorul de servicii internet e posibil să vă anuleze contractul.
  - Este posibil să fiți acționați în justiție pentru daune și să fiți nevoiți să plătiți compensații financiare părții vătămate.

Probleme etice

- **Tipuri de licențe**
  - *Licența monopost:* când cumpărați programul obțineți dreptul de a instala și folosi programul doar pe un singur computer.
    - Dacă achiziționați programul online, îl plătiți, în descărcați iar apoi îl înregistrați la producător care vă va trimite un *număr de licență* numit *și cheie de produs.* Aceasta vă va permite activarea produsului cumpărat.
  - *Licența de volum* sau *de rețea:* pentru organizații cu multe computere.
    - Departamentul IT primește programul pe un mediu de stocare și îl copiază într-un folder din rețea de unde va fi instalat pe mai multe computere.
      - Instalarea se va face pe toate computerele utilizând aceeași cheie de produs.
    - Opțiune rentabilă pentru că reduce timpul de instalare și costurile.

Probleme etice

- Licența per locație: oferă dreptul de a utiliza programul în rețelele aflate într-o singură locație fără limită de utilizatori.
  - Mai scumpă decât o singură copie dar mai ieftină decât suma copiilor individuale necesare.
- *Licențele Software sub formă de serviciu (SaaS – **S**oftware **a**s **a** **S**ervice)* vă permit utilizarea unui program în rețea, fie aceasta intranetul organizației sau internetul.
  - Furnizorul acestor servicii se numește *ASP (**A**pplication **S**ervice **P**rovider).*
  - Trebuie să utilizați un cont și o parolă valide înainte de a accesa programul.
  - Odată ce contractul SaaS a expirat, nu mai puteți accesa programul decât dacă optați pentru o prelungire a acestuia.

Probleme etice

- **Alte tipuri de licențiere**
  - ***Shareware***: versiuni de încercare ale programelor pe care le puteți descărca gratuit. Aceste programe au funcționalitate redusă sau expiră după o anumită perioadă de timp.
    - Dacă sunteți mulțumit, plătiți o sumă modică și înlăturați restricțiile.
  - ***Freeware***: programe absolut gratuite ce pot fi partajate cu alte persoane fără restricții.
  - **Programe la pachet** (***Bundles***): cumpărarea unui PC include poate include licența pentru SO dar și unele versiuni de încercare pentru alte programe.
    - Unele programe trebuie înregistrate online sau plătite pentru versiunea completă.
  - **Programe Premium**: pachete speciale de programe în care cu o singură cheie de produs activați toate programele din pachet.

Probleme etice

- **Open Source**: codul sursă este „deschis”, adică poate fi accesat, particularizat și schimbat.
  - Există totuși restricții în sensul că îl puteți partaja dar nu puteți pretinde drepturi de autor sau bani șu nu puteți transforma sursele în unele private.
- Prin orice modalitate ați obține software, este responsabilitatea dvs. de a respecta regulile de licențiere.
  - Când achiziționați software licențiat, veți fi notificați de către furnizor despre actualizări, pe care le veți putea descărca gratuit.
  - Dacă nu aveți o licență validă, violați drepturile de autor ale producătorului și puteți fi dați în judecată.
  - Citiți întotdeauna *Acordul de licență cu utilizatorul final* – **EULA** (***E**nd **U**ser **L**icense **A**greement*) în momentul instalării și apoi conformați-vă acestuia.

Probleme etice

- **Creative Commons (CC)**
  - este o organizație non-profit care pune la dispoziție șase tipuri diferite de licență pentru persoanele care vor să împărtășească cu alții munca lor creativă sau cunoștințele pe care le au, dar să păstreze totodată dreptul de autor.
    - nu înlocuiesc dreptul de autor dar îl ajută pe deținătorul acestuia să monitorizeze felul în care munca lui creativă este distribuită sau utilizată.
  - Oferă metode standard de a permite accesul la munca creativă păstrând restricțiile legilor referitoare la drepturile de autor, asigurând vizibilitatea și recunoașterea deținătorului acestora.
  - Deținătorul dreptului de autor poate utiliza ce tip de licență dorește.

Probleme etice

Atribuire	Oricine va putea distribui, modifica și combina materialul dvs.,atâta timp cât **sunteți menționat ca autor** al materialului originar.
Atribuire – Fără modificări	Oricine poate distribui materialul în **scopuri comerciale sau non-comerciale**, dar trebuie păstrat în **forma originală**, iar dvs. **sunteți recunoscut ca autor**.
Atribuire – Necomercială Distribuire în condiții identice	Oricine va putea distribui, modifica și combina materialul dvs. în **scopuri necomerciale** cu condiția de a vă **recunoaște drepturile de autor** al materialului originar și de a **licenția noua lucrare în exact aceiași termeni**.
Atribuire – Distribuire în condiții identice	Oricine va putea distribui, modifica și combina materialul dvs. **în scopuri comerciale** cu condiția de a vă **recunoaște drepturile de autor** al materialului originar și de a **licenția noua lucrare în exact aceiași termeni**.
Atribuire – Necomercială	Oricine va putea distribui, modifica și combina materialul dvs. în **scopuri necomerciale** cu condiția de a vă **recunoaște drepturile de autor** al materialului originar **fără obligația de a licenția noua lucrare în exact aceiași termeni.**
Atribuire – Necomercială Fără modificări	Oricine va putea descărca și distribui lucrările originale cu condiția de a vă **recunoaște drepturile de autor** al materialului originar **acesta neputând fi modificat sau utilizat în scopuri comerciale**.

Probleme etice

- Există și licențe cu toate drepturile garantate, în cazul în care lucrările sunt considerate ca fiind de domeniu public.
  - Proprietarul renunță la toate drepturile asupra materialelor originale.
- Gestionând felul în care materialele cu drepturi de autor pot fi partajate sau utilizate:
  - Organizațiile pot oferi informații publicului larg fără a-și face griji, în majoritatea cazurilor, privind violarea unor legi ce privesc dreptul de autor.
  - Informațiile pot fi actualizate și distribuite într-o manieră echitabilă atât pentru deținătorul drepturilor de autor, cât și pentru organizația care folosește licența respectivă.

Probleme etice

- **Cenzura și filtrarea**
  - Nu există un organ de conducere care să monitorizeze conținutul materialelor publicate online.
    - există multe „zone gri” între un material bun și un altul rău, fapt ceea ce a dus la apariția cenzurii cu scopul protejării utilizatorilor internetului.
  - **Filtre și restricții**
    - Există aplicații care permit controlul asupra tipurilor sau cantității de conținut ce poate fi vizualizat.
    - Unele site-uri sociale pot de asemenea bloca anumite mesaje sau postări care au un conținut îndoielnic sau inacceptabil.
      - Furnizorii de internet (ISP), pot și ei bloca aceste tipuri de mesaje odată ce interceptează conectarea la o anumită rețea socială.
      - Alte site-uri pot avea un moderator, care avertizează utilizatorii când conversațiile încep să devină necorespunzătoare.

Probleme etice

- Aceste instrumente sunt similare cu cenzura cu diferența că, ele nu afectează proprietarul conținutului.
  - Aceste poate în continuare să împărtășească informația respectivă.
- *Lista neagră*: utilizatorilor trecuți în această listă i se va refuza accesul la un anumit serviciu. Dacă dintr-un motiv sau altul vă aflați pe această listă:
  - Contactați furnizorul de internet și oferiți explicațiile necesare scoaterii din listă.
  - Ar putea fi nevoie de o scrisoare oficială prin care să se solicite scoaterea de pe lista neagră, sau chiar de schimbarea ISP-ului dacă acesta nu vă poate rezolva.
- Nu este clar care informații pot fi considerate ofensatoare sau periculoase ?
- O problemă este și atunci când cineva schimbă în mod nelegitim configurația acestor instrumente de control al accesului stabilită de organizație.
- Guvernele anumitor țări au puterea de a cenzura un anumit conținut în întreaga țară și controlează toate computerele conectate la internet.

Probleme etice

- **Practici de evitat**
  - Din motive morale, etice și legale.
  - **Plagiatul**
    - Este atunci când cineva folosește informațiile oferite de o altă persoană și le prezintă ca și cum i-ar aparține, cuvânt cu cuvânt sau cu schimbări minore.
    - Această practică este considerată furt.
    - Când utilizați informații de pe internet, folosiți informațiile originale și citați sursa materialului pentru a vă asigura că sunteți în legalitate.
    - Prin recunoașterea faptului că împrumutați conținutul și furnizați informațiile sursei, în cele mai multe cazuri, veți evita să fiți acuzat de plagiat.

Probleme etice

- **Calomnia**
  - Calomnia este o formă de defăimare a unei persoane sau organizații.
    - Calomnia în formă orală este numită în engleză *slander*.
    - Calomnia în formă scrisă este numită în engleză *libel*.
  - Cel mai înțelept lucru pe care îl puteți face, atât în mediul online, cat și în afara lui, este să tratați calomniile precum zvonurile:
    - Nu le începeți, nu le ascultați și nu le răspundeți.

Probleme etice

- **Pirateria**
  - Este asociată cu încălcarea drepturilor de autor, în sensul că lucrările originale au fost reproduse sau modificate fără permisiunea proprietarului.
  - Apare când un element este partajat cu alte persoane fără compensație materială pentru autor.
  - Dacă descărcați materiale cu drepturi de autor puteți fi dat în judecată.
  - Pirateria este delict federal în Statele Unite dacă curtea stabilește că aceasta s-a produs având ca scop clar obținerea de foloase materiale.
    - Pedeapsa penală poate ajunge până la zece ani de închisoare.
  - Pentru a vă proteja împotriva oricăror acuzații de piraterie, fie ea chiar și accidentală achiziționați întotdeauna programe de la comercianți cu renume în domeniu.

Probleme etice

- **Comportamentul necorespunzător**
  - Farsele (*pranks*) pot fi dureroase și ar trebui evitate.
  - Intimidarea (*bullying*) în mediul online are loc când una sau mai multe persoane sunt agresate în mod constant și deliberat prin postări sau mesaje ostile sau răutăcioase.
  - Evitați să insultați oamenii (*flaming*). Este considerat insultă:
    - Un email sau un mesaj online în care este atacat personal destinatarul mesajului.
  - Dacă ești insultat, cel mai bine este să ignori.
    - Dacă răspunzi, se poate ajunge la un adevărat „război al insultelor” (*flame war*).

Probleme etice

- Evitați să trimiteți mesaje spam/nesolicitate.
- Nu distribuiți informații personale despre alții, chiar dacă părțile implicate se cunosc între ele.
  - Dacă cineva v-a oferit informații confidențiale, respectați intimitatea acestuia și păstrați aceste informații doar pentru dumneavoastră.
  - Evaluați cu atenție materialele pe care le postați online. Manifestați discreție.
- Nu ridiculizați și nu disprețuiți opiniile altora.
- Dacă doriți să creați diferite documente ale căror informații au ca scop uzul online, oferiți fapte și surse care vin în susținerea informațiilor folosite.
  - Mențineți unui ton respectuos și stabiliți-vă mesajul în funcție de utilizatori.
- Regula de aur: comportați-vă cu ceilalți la fel cum ați dori să se comporte aceștia cu dumneavoastră, atât în mediul online, cât și în afara lui.

Probleme etice

Practicarea unei bune cetățenii online

- Normele de bun simț din în viața reală, urmați-le și online.
- Verificarea gramaticală să nu fie singura unealtă în comunicare.
- Fiți prudenți când folosiți abrevieri sau acronime.
- Țineți întotdeauna cont de destinatarul mesajului.
- Alegeți o formă de comunicare adaptată scopului discuției.
- Nu vă implicați emoțional în comunicare (mai ales negativă).
- Apelați la bunul simț în legătură cu ceea ce vreți să postați.

Exercițiu 1 - 1

În acest exercițiu vom explora cele nouă elemente ale comunicării digitale și apoi vom discuta cu ceilalți despre regulile generale și ce impact ar putea să producă. Va trebui să folosiți Google Chrome și elementele sale automate de traducere dacă doriți să vizualizați paginile indicate mai jos în limba română.

1. Porniți un browser web și, în bara de adrese, tastați: `www.bing.com` și apăsați **Enter**.
2. În câmpul de căutare tastați: `9 elements of digital citizenship` și apăsați **Enter**.
3. Faceți clic pe legătura www.digitalcitizenship.net/Nine_Elements.html.
4. Citiți conținutul acestei pagini și apoi deschideți o discuție cu privire la fiecare dintre aceste puncte.
   - Cât de relevante sunt aceste puncte pentru comportamentul online?
   - Există zone în care credeți că există mai multe recomandări decât ar fi necesar?
   - Ce alte subiecte credeți că ar mai trebui incluse sau tratate mai elaborat în această listă?

Exercițiu 1 - 2

6. Navigați înapoi la pagina cu rezultatele căutării și accesați alte link uri pentru a vizualiza informația oferită acolo.
7. În câmpul de căutare, tastați : `being a good online citizen` și apăsați **Enter**.
8. Ce rezultate ați obținut de această dată? Faceți clic pe câteva dintre ele pentru a le citi conținutul și pentru a decide dacă acestea sporesc informațiile deja citite în paginile dedicate Cetățeniei Digitale din acest manual.
9. După navigarea pe câteva alte site uri închideți browser-ul.

Protejarea computerului și a datelor

- **Furtul**
  - achiziționați sisteme care închid computerele în dulapuri speciale sau puteți folosi cabluri de oțel pentru a le lega de birou.
  - Camerele de supraveghere sunt eficiente în spații cu un număr mare de computere cum ar fi birourile centrale sau incintele serverelor.
  - Nu lăsați dispozitivele portabile nesupravegheate nici un moment atunci când vă aflați în zone publice.

Protejarea computerului și a datelor

- **Pierderea datelor**
  - Puteți pierde datele ca rezultat al acțiunilor criminale în mediul online, al unor defecțiuni ale echipamentelor, al unor pene de curent, ștergeri accidentale, furturi sau distrugeri de echipamente ori din cauza unor angajați distrați.
  - Dacă oferiți un serviciu important, e necesar un plan de urgență pentru a putea face față unei pierderi în masă a datelor.
  - Aveți grijă de dispozitivele portabile când sunteți în locuri publice.
    - Sincronizați datele de pe dispozitivele mobile cu servere de backup.
  - Pentru a reduce posibilitatea ca cineva să poată schimba fișierele de date, luați în considerare adăugarea unei parole fiecărui fișier sau ștergeți orice drepturi partajate asupra fișierelor sau a folderelor.

Protejarea computerului și a datelor

- **Securitatea datelor**
  - Un *hacker* încearcă să obțină controlul asupra computerului dvs. pentru:
    - a fura informații pe care să le vândă apoi,
    - a distruge date ce ar cauza companiei incapacitatea de a furniza produse, servicii sau proiecte la timp,
    - schimba informații, acest lucru aducând o imagine defavorabilă și o reputație negativă companiei dumneavoastră.
  - O modalitate eficientă de a vă proteja datele este parolarea lor.
    - Utilizați o parolă logică pentru dvs. dar dificil de ghicit pentru alții.
    - Nu utilizați nume, date de naștere, numere de telefon sau alte date personale.
    - Folosiți o combinație de litere mari și mici, numere și caractere speciale.

Protejarea computerului și a datelor

- Schimbați-vă parola cu regularitate
- Ca să nu rețineți prea multe parole folosiți prin rotație patru sau cinci.
- Folosiți parole diferite pentru protejarea fișierelor și pentru internet.
- Utilizați cu precauție reținerea parolelor de către browser.
- Instalați instrumente specializate pentru protecția echipamentelor de calcul.
- Angajați consultanți de securitate pentru a vă audita infrastructura IT.

Protejarea computerului și a datelor

- **Copii de siguranță**
  - Faceți copii de rezervă a datelor, pe dispozitive de stocare amovibile.
  - Frecvența copierilor de rezervă e direct proporțională cu importanța lor.
  - Încurajați utilizatorii care stochează datele pe discurile locale, să-și facă copii zilnice ale acestora, pe server sau copii de siguranță independente.
  - Educați utilizatorii să-și salveze frecvent fișierele în care lucrează.
  - Includeți copierea de siguranță în planul de măsuri în caz de calamități.
  - Multe companii stochează copiile de siguranță în cloud.
    - Asigură astfel stocarea copiilor de siguranță în altă locație și recuperarea lor din orice altă locație, dacă există conectivitate la internet.

Protejarea computerului și a datelor

- **Identificarea programelor periculoase**
  - **Spyware/Adware/Cookies**
    - *Spyware:* aplicații care sunt plasate în mod secret în sistemul utilizatorului și care adună informații personale sau private fără cunoștința acestuia.
      - Poate fi plasat în computer de către un virus sau o aplicație din internet.
      - Monitorizează activitatea dvs. în internet și trimite creatorului său informații despre paginile web accesate, adresele de e-mail etc. cu scopuri malițioase.
    - *Adware:* aplicații care afișează sau descarcă reclame în mod automat.
    - *Cookies*: fișiere text în care paginile web vizitate își stochează informații.
      - În general nu sunt periculoase dar pot stoca nume de utilizatori și parole online.
      - Rețin activitățile browserului și configurările pentru anumite pagini web.

Protejarea computerului și a datelor

- **Malware**
  - Se referă la acele programe sau fișiere a căror intenție specifică este de a afecta sistemele informatice.
  - Este o formă electronică de vandalism care poate avea implicații globale.
  - Include viruși, viermi și cai troieni.
    - *Viermii:* programe cu capacitatea de a se auto-replica. Consumă resursele de sistem și de rețea și se pot răspândi în mod automat de la un computer la altul.
    - *Cal troian*: program conceput pentru a permite accesul de la distanță a unui hacker la un sistem informatic țintă.

Protejarea computerului și a datelor

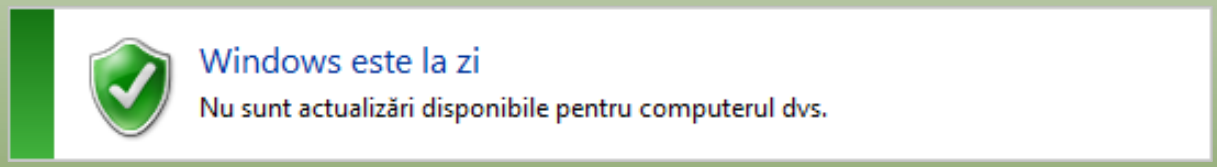
- **Descărcarea**
  - Se referă la salvarea unor programe sau fișiere din internet pe discul local.
  - Dacă instalați programe direct din internet, descărcare devine transparentă.
    - Fișierele executabile pot fi infectate cu malware. Verificați-le cu antivirusul.
    - E recomandabil să aveți un folder dedicat descărcărilor, sistematic verificat.
  - Citiți cu atenți informațiile din ferestrele de dialog, mai ales înainte de OK.
    - Citiți EULA pentru a vedea cum vor fi utilizate datele colectate din computer.

Protejarea computerului și a datelor

- **Configurarea unui paravan personal de protecție**
  - Protejează computerul împotriva comunicațiilor potențial periculoase și împotriva accesului neautorizat.
  - Paravanele personale de protecție sunt aplicații.
    - Windows include un paravan de protecție pre-instalat, dar utilizatorul poate achiziționa alte paravane de protecție dacă are anumite cerințe mai speciale.
  - Monitorizează, cererile de comunicare cu computerul care provin din internet, precum și cererile de comunicare cu exteriorul care provin aplicații.
  - Poate bloca aceste comunicări dacă nu recunoaște că un anumit program are permisiunea de a trimite și primi cereri de comunicații.
  - Puteți verifica și ajusta setările paravanului personal de protecție prin selectarea Paravan de protecție Windows din Panoul de control.

Protejarea computerului și a datelor

- **Actualizări**
  - Sunt importante pentru a proteja SO în fața amenințărilor de securitate.
  - Noi viruși sunt creați în mod regulat, iar unii dintre aceștia sunt concepuți pentru a exploata vulnerabilitățile de securitate din Windows.
  - Microsoft lansează actualizări în mod regulat pentru a proteja computerele împotriva acestor amenințări.
    - Când primiți o notificare de actualizare Windows puteți verifica ce actualizări sunt disponibile și le puteți instala pe acelea care abordează probleme de securitate.



Protejarea computerului și a datelor

- **Fișiere reziduale**
  - Pot rămâne pe computer în urma dezinstalării unui program.
  - Nu sunt periculoase, ele pot conține informații personale care pot fi exploatate în cazul în care computerul dvs. este compromis.
  - După ce ați dezinstalat un program, examinați hard discul pentru a verifica dacă a mai rămas vreun folder nesters al programului respectiv.
    - Dacă găsiți astfel de foldere le puteți șterge manual.
  - Unele programe să nu se dezinstalează complet acestea putând lăsa anumite înregistrări eronate în Windows Registry.
    - Windows Registry este o bază de date din Windows care ține evidența setărilor de configurare și a programelor instalate.
    - Înregistrările parțiale sau eronate în Windows Registry pot provoca probleme de performanță.

Protejarea computerului și a datelor

- Fișiere reziduale pot rămâne și după ștergerea unor fișiere de date.
  - Fișierele șterse de pe hard disc sunt stocate în Coșul de reciclare. Acesta trebuie golit în cazul în care conține fișiere confidențiale.
- Dacă donați un computer vechi, care a păstrat în trecut informații cu caracter personal, ar trebui să utilizați un utilitar numit *shredder* care să distrugă toate datele de pe hard disc.
  - Formatarea discului face ca spațiul de stocare să devină disponibil încă o dată, dar nu distruge datele stocate pe acesta.
- Dacă utilizați dispozitive de stocare portabile, fiți mereu atenți în cazul în care aceste dispozitive conțin informații confidențiale.
  - Nu le lăsați în locuri unde utilizatori neautorizați ar putea să le acceseze.

Protejarea computerului și a datelor

- **Cookies**
  - Un cookie este un mic fișier text salvat pe hard disc de către un anumit site web pentru a permite schimbul de informații între computer și acesta.
  - În general, cookie-urile nu sunt dăunătoare sau periculoase și nu conțin informații personale deși pot fi utilizate pentru autentificare.
  - Dezavantajul acestor cookie-uri este că oricine are acces la computerul și contul dvs. de utilizator, se va putea conecta la conturile dvs. online la care autentificarea se bazează pe cookies.
  - Un alt dezavantaj al cookie-urilor este acela că pot fi folosite pentru a identifica anumite obiceiuri și interese de cumpărare.
  - Cookie-urile pot fi eliminate prin curățarea lor din browserul web folosind instrumentele specifice fiecărui browser.

Protejarea computerului și a datelor

- **Viruși**
  - Virusul este un program care preia controlul operațiunilor de sistem și produce daune sau distruge date.
    - Toți virușii informatici sunt creați de om și sunt adesea concepuți să se răspândească la alți utilizatori de computere.
    - Pot fi transferați prin atașamente de email, programe sau fișiere descărcate, și prin utilizarea discurilor infectate, CD-uri sau flash drive-uri.
  - Un virus poate:
    - Afișa mesaje inofensive pe ecran.
    - Utiliza toată memoria, încetinind sau afectând toate celelalte procese.
    - Corupe sau distruge fișiere de date.
    - Șterge conținutul unui întreg hard disc.

Protejarea computerului și a datelor

- Virușii sunt orientați spre sistemele de operare Windows și Mac OS.
  - Un tip comun de virus care vizează rețelele companiilor vine sub forma unui atașament de email și se răspândește cu ajutorul listei de contacte.
    - Acest tip de virus de email nu deteriorează date, dar consumă resursele de rețea datorită mesajelor generate și transmise automat de pe fiecare computer al companiei pe care a fost deschis atașamentul virusat.
  - Unii viruși sunt mult mai distructivi.
    - Pot șterge fișiere de date, pot defecta programe și pot rescrie înregistrări din Windows Registry.
    - Pot face un computer complet inutilizabil și pot corupe toate datele sale.

Protejarea computerului și a datelor

- **Program anti-virus**
  - Scanează atașamentele de email și fișierele în vederea detectării și eliminării oricăror viruși cunoscuți descoperiți în computer.
  - Toate versiunile de antivirus includ actualizări ale definițiile virușilor.
  - Dacă computerul dvs. este infectat cu un virus, chiar dacă programul antivirus detectează prezența acestuia, este posibil să nu-l poată elimina complet până când nu efectuați o scanare completă a computerului.
    - Dacă nu poate curăța virusul, va carantina fișierele afectate.
    - Este extrem de important să aveți un program antivirus instalat pe computerul dvs. configurat pentru a rula atunci când computerul pornește.

Protejarea computerului și a datelor

- **Manifestări ce pot indica prezența unui virus**:
  - Mesaje, solicitări, sau afișări pe ecran pe care nu le-ați mai văzut înainte.
  - Funcționare lentă a computerului sau probleme în folosirea anumitor programe.
  - Anumite aplicații nu mai funcționează, sau încep să ruleze automat.
  - Sunete aleatorii sau muzică pe care nu le-ați mai auzit până acum.
  - Numele discurilor sau al fișierelor par a se fi schimbat.
  - Computerul pare să conțină mult mai multe sau mai puține fișiere decât de obicei.
  - Mesaje de eroare care indică faptul că lipsește un fișier, de obicei un fișier program.
  - Primiți mesaje de email, cu atașamente, de la persoane pe care nu le cunoașteți.
  - Primiți multe mesaje cu atașamente de la persoane pe cunoscute, dar linia de subiect are prefixul „RE:” sau „FW” chiar dacă nu ați trimis nimic înainte acelor persoane.

Protejarea computerului și a datelor

- Dacă sunteți îngrijorat antivirusul nu detectează toți virușii:
  - Scanați toate dispozitivele portabile, chiar dacă nu există programe pe ele.
  - Nu deschideți atașamentele fără o scanare prealabilă.
  - Navigați la site-ul web al antivirusului și executați o scanare on-line.
    - Utilizând cea mai nouă versiune a programului, scanarea online poate detecta viruși care au scăpat scanării cu versiunea instalată local a programului.
    - Actualizați des antivirusul sau configurați-l să se actualizeze automat.
  - Puteți apela la un specialist IT, care va fi capabil să lucreze cu dvs. la scanarea unităților de computer împotriva potențialilor viruși, și să decidă pe baza rapoartelor eliminarea sau izolarea în carantină a virușilor.

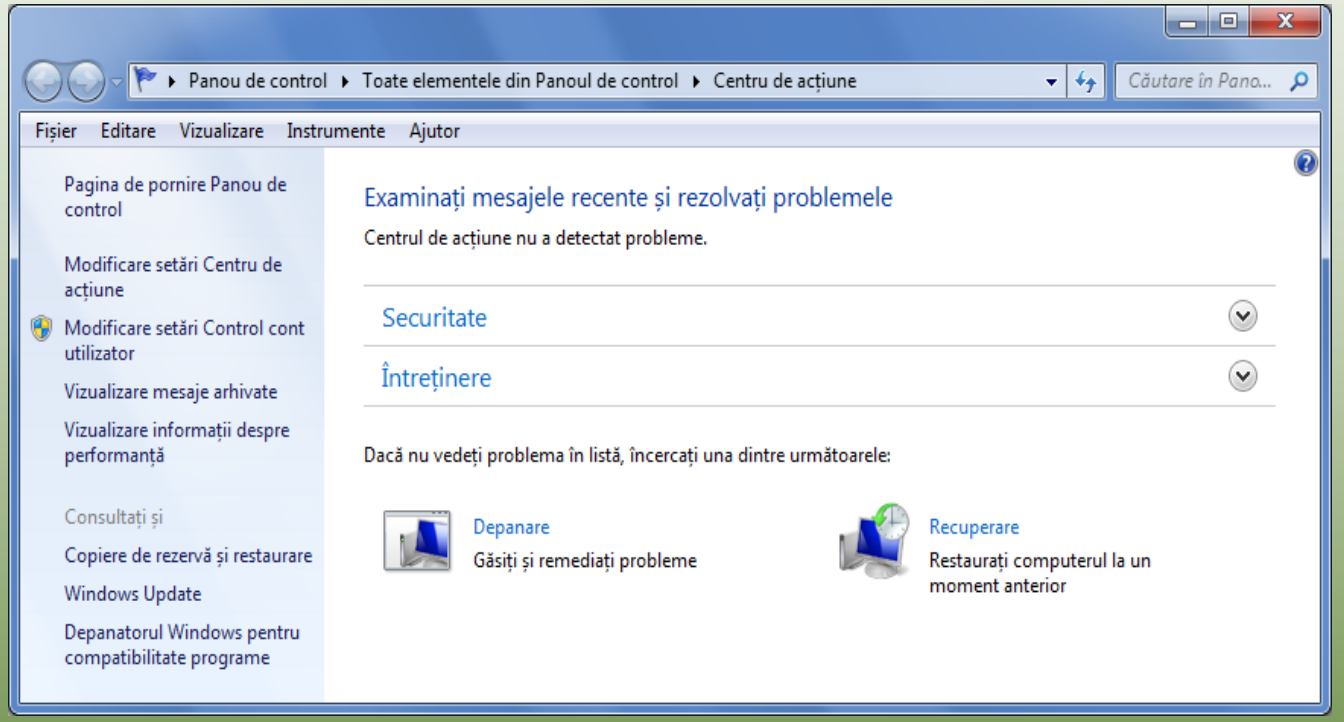
Protejarea computerului și a datelor

- **Eliminarea virușilor din computer**
  - Când este identificată un malware, programul antivirus vă va notifica și vă va oferi opțiunea de a-l izola în carantină sau de a-l elimina complet.
    - Dacă optați pentru carantinare, fișierele infectate vor fi mutate într-o zonă asigurată din care nu vor mai putea infecta și alte fișiere.
    - Dacă optați pentru eliminare, fișierul infectat va fi șters definitiv.
    - Dacă virusul nu poate fi eliminat, fișierul infectat va fi carantinat.
      - Notați-vă numele virusului și după scanare căutați pe site-ul web al antivirusului pentru a găsi un instrument specializat în eliminarea virusului respectiv.
  - Vizitați istoricul antivirusului și examinați fișierele din zona de carantină.
    - Ștergeți fișierele cu viruși care pot exista în continuare pe dispozitiv.

Exercițiu 2 - 1

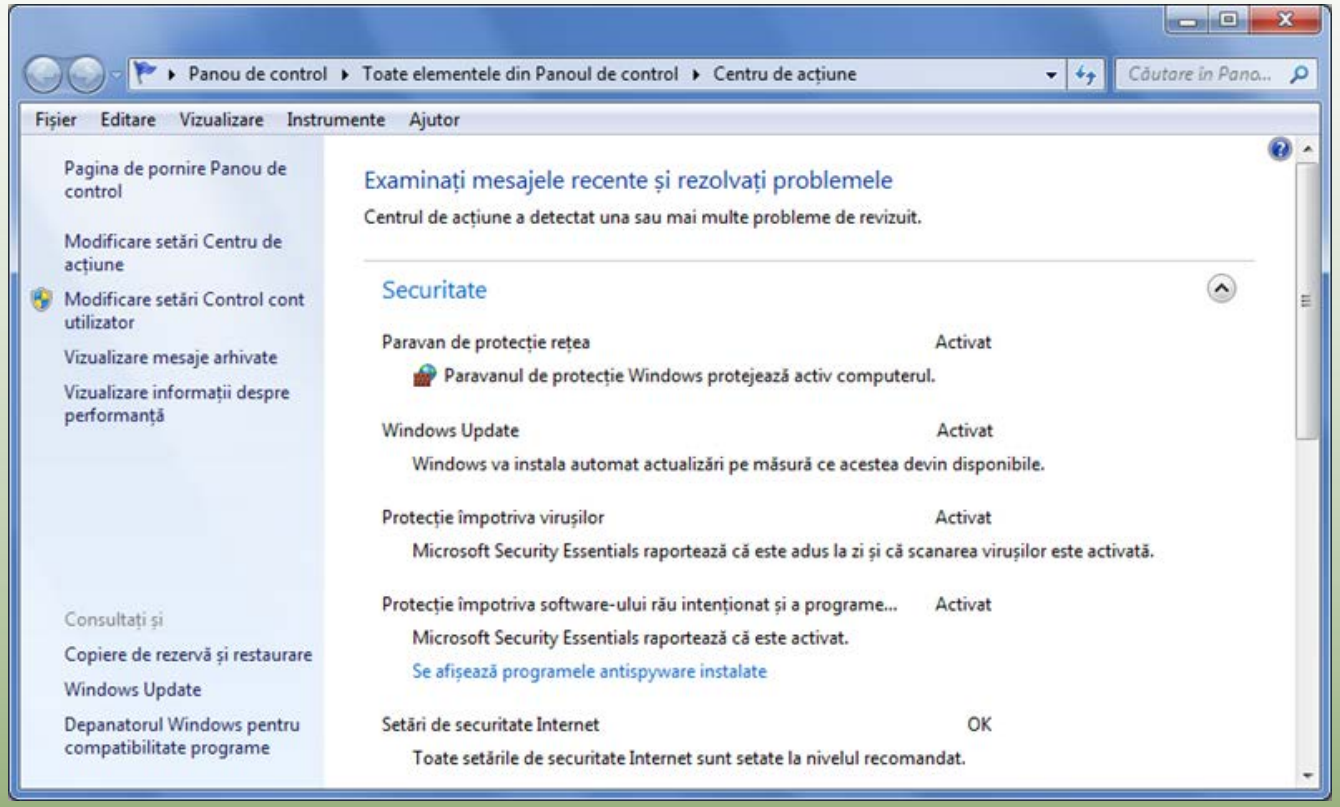
În acest exercițiu veți examina setările de securitate de pe propriul computer.

1. Deschideți **Panou de Control**, faceți clic în câmpul de **Căutare în Panoul de control** și tastați: `starea securității`.
2. Faceți clic pe linkul **Verificați starea securității**.



Exercițiu 2 - 2

3. Faceți clic pe săgeata din dreapta linkului **Securitate**.



Informațiile afișate pe ecran vor varia în funcție de programele care au fost instalate pe propriul computer pentru protecție.

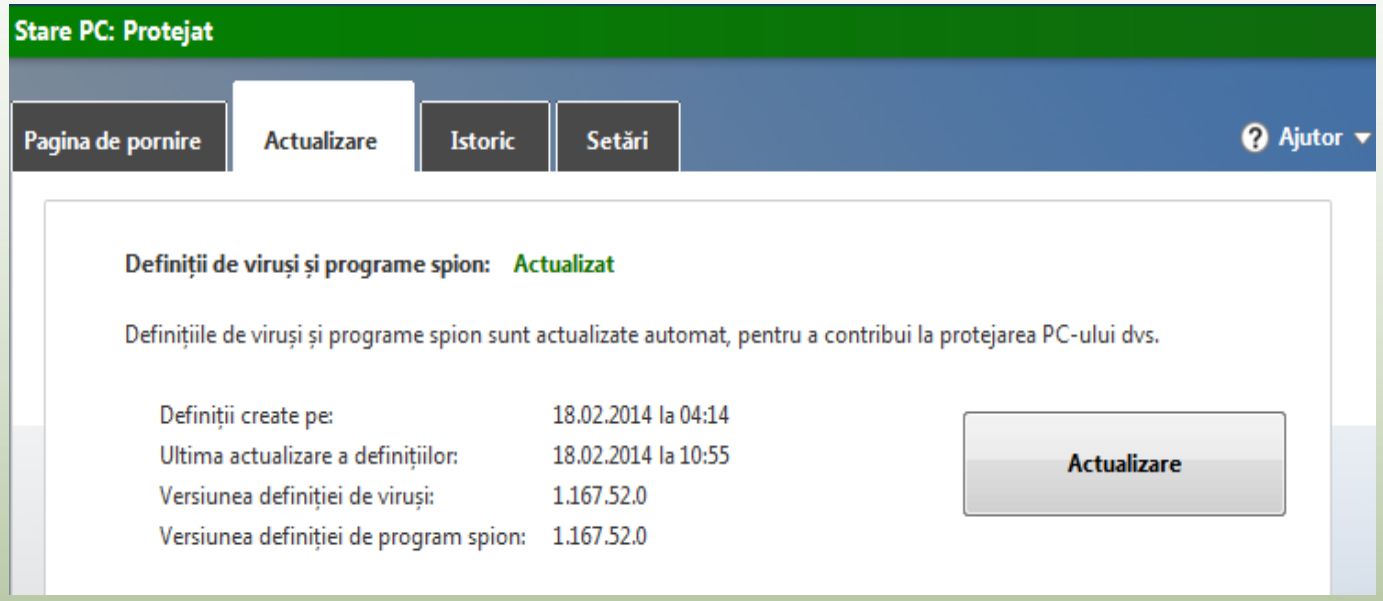
Exercițiu 2 - 3

4. Rulați prin listă pentru a vedea care opțiuni sunt active pe computerul dumneavoastră.
5. Închideți fereastra.

   Veți afla acum despre programul anti virus pus la dispoziție gratuit de către Microsoft numit *Microsoft Security Essentials*. Dacă există un alt program anti-virus instalat pe computerul propriu, activați acel program prin acționarea meniului Start pentru a i vizualiza opțiunile. În acest caz urmăriți doar pașii care urmează și încercați să descoperiți caracteristicile similare din programul instalat pe computerul dumneavoastră.
6. Faceți clic pe **Start** și tastați în câmpul de căutare: `security essentials`.
7. Faceți clic pe elementul **Microsoft Security Essentials** aflat în partea de sus a meniului Start.

Exercițiu 2 - 4

8. Faceți clic pe fila **Actualizare**.



În funcție de configurația programului, trebuie să verificați actualizările periodic pentru a vă asigura că protecția dvs. anti virus este la zi. Ecranul prezentată anterior indică faptul că actualizările sunt configurate să se realizeze în mod automat. În mediile corporatiste, computerele sunt configurate să caute actualizări în mod automat în momentul în care utilizatorul se conectează la rețea.

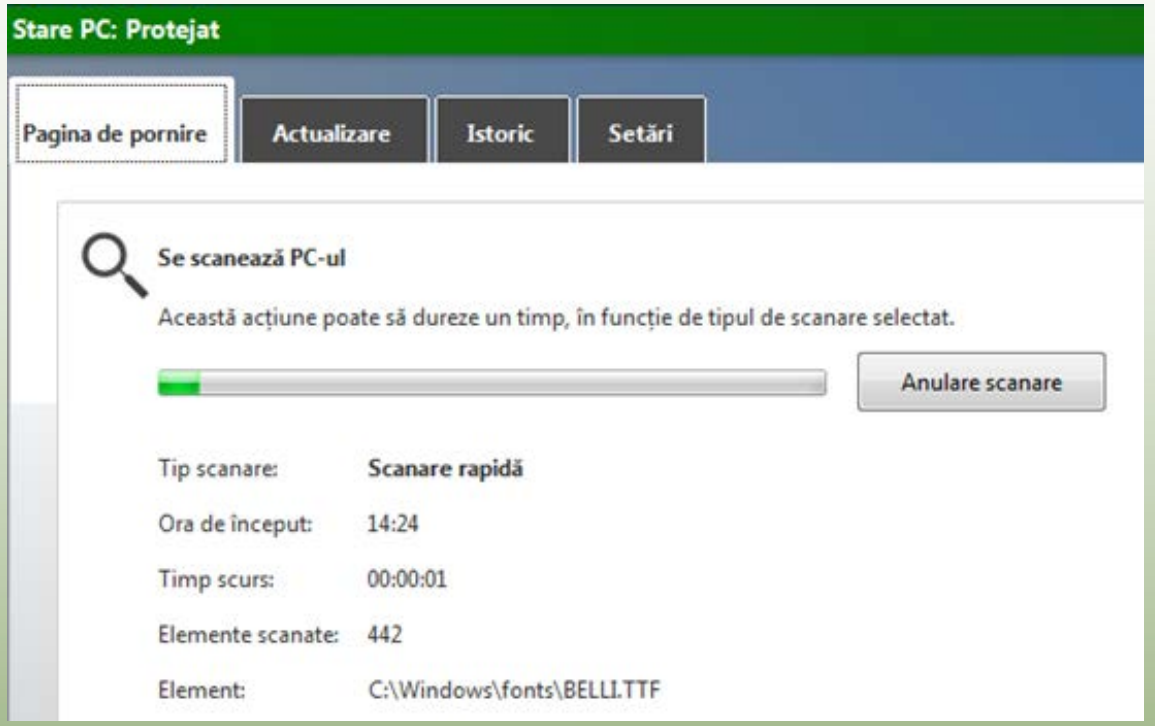
Exercițiu 2 - 5

9. Faceți clic pe fila Pagina de pornire. Asigurați-vă că Opțiuni de scanare sunt setate pe Rapid și apoi faceți clic pe Scanare acum.

   Durata de scanare depinde de data la care a fost făcută ultima actualizare și de cantitatea de date existentă pe hard disc.

10. În funcție de cum vă permite timpul. Permiteți scanării să finalizeze procesul, sau faceți clic pe Anulare scanare pentru a încheia această operațiune.

11. Închideți programul anti virus.



Protecția muncii

- **Siguranța și confortul muncii**
  - Leziunile de stres repetitiv (RSI – ***R****epetitive* ***S****train* ***I****njury*) devin tot mai frecvente datorită perioadelor îndelungate petrecute la computer.
    - RSI apar gradual și sunt cauzate de prea multe mișcări repetate fără întrerupere în timpul unor activități.
    - RSI apar în general la mâini și încheieturile acestora precum și la brațe, dar pot afecta și gâtul ori alte articulații cum sunt coatele.
  - Pentru prevenirea RSI utilizatorii pot folosi mobilier ergonomic și tehnici specifice de utilizare a computerului în siguranță.
    - *Ergonomi*a este știința care se ocupă cu studiul condițiilor de muncă în vederea realizări unei adaptări optime a omului la acestea în condiții de maximă siguranță și confort.

Protecția muncii

- Pentru a preveni RSI:
  - Stați pe un scaun cu sprijin lombar, cotiere și înălțime ajustabilă.
  - Folosiți o tastatură ergonomică.
  - Înclinați monitorul în sus cu 10 grade pentru a preveni durerile de gât.
  - Folosiți un suport căptușit pentru a vă sprijini încheieturile mâinilor.
  - Poziționați monitorul la o distanță de 60 până la 75 cm față de ochi.
  - Ajustați rezoluția monitorului pentru ca textul să suficient de clar.
  - Asigurați-vă că ecranul monitorului nu pâlpâie (rata de refresh min. 72 Hz).
  - Nu priviți ecranul computerului pentru perioade lungi de timp.

Protecția muncii

- Dacă lucrați la un computer timp de câteva ore pe zi:
  - Niciodată nu lucrați la computer fără pauze regulate.
  - Suprafața de lucru trebuie să fie stabilă, cu obiectele în poziție orizontală.
  - Monitorul și tastatura trebuie să fie poziționate exact în față.
  - Partea de sus a monitorului trebuie să cu 5 până la 7 cm deasupra ochilor.
  - Nu trebuie să existe reflecții pe ecran.
  - Ar trebui să aveți o sursă de lumină direct deasupra monitorului.
  - Poziționați documentele, paralel cu monitorul, într-un suport special.
  - Așezați-vă confortabil, poziționați antebrațele cu încheieturile mâinilor drepte si aliniate orizontal și coatele apropiate de corp.
  - Păstrați toată talpa pe podea iar coapsele și antebrațele paralele cu podeaua.

Protecția muncii

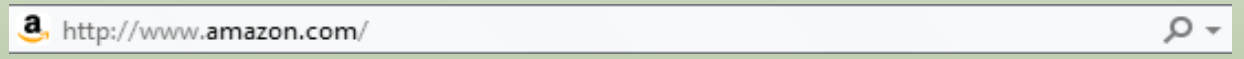
- Tastatura trebuie să se afle într-o astfel de poziție încât brațele să nu obosească în timpul tastării.
- Același lucru este valabil și pentru mouse.
- Atunci când tastați, încercați să nu îndoiți încheietura mâinii.
- Dacă simțiți un disconfort în încheieturi, brațe sau degete atunci când folosiți un mouse tradițional, încercați un mouse mai mare, un trackball sau un dispozitiv care utilizează tehnologia tactilă.
- Aceste recomandări sunt valabile și pentru utilizatorii de notebook-uri.
  - Dacă sprijiniți notebookul pe picioare, asigurați-vă că aveți poziția corectă și încercați să folosiți un suport sau o platformă de susținere atunci când lucrați.

Protecția în mediul online

- Fiți atent în mediul online, pentru a vă proteja informațiile personale.
- Asigurați-vă că parolele pe care le folosiți sunt cât mai puternice.
  - Schimbați-vă periodic parolele pentru a vă asigura o protecție continuă.
- Pentru site-uri la care vă înregistrați pentru a revenii ulterior, folosiți o adresă alternativă de web email.
  - Reduce numărul de mesaje nedorite în contul dvs. principal de email.
  - Folosiți contul dvs. principal de email doar pentru acele site-uri de la care faceți achiziții concrete.

Protecția în mediul online

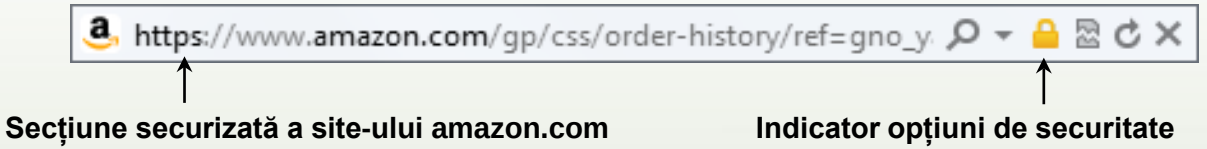
- **Cumpărăturile online**
  - Siguranța pe care o simțiți făcând tranzacții sau banking online, va determina cât de multe cumpărături online veți face.
  - Dacă o companie are o ofertă ce pare prea bună pentru a fi adevărată:
    - Fiți precauți ca și când cineva v-ar face aceeași ofertă în mediul offline.
  - Verificați dacă compania are incluse opțiuni de securitate pentru site.



    - Pe o pagină unde trebuie să furnizați date personale adresa se schimbă:

    - ***https*** înseamnă că sunteți în partea securizată a site-ului, unde puteți introduce date personale sau puteți face tranzacții financiare în siguranță.

Protecția în mediul online



- Când introduceți informațiile personale pe un site, faptul că vă conectați printr-o conexiune securizată este indicat în bara de adrese (https și).
  - *Soclu de conexiune securizat* (***SSL*** - ***S****ecure* ***S****ocket* ***L****ayer*) indică faptul că transferul informațiilor se va face folosind o tehnologie de criptare.
  - Înainte de expediere, informația trebuie criptată cu ajutorul unei chei de criptare publice (a destinatarului) textul acestei informații devenind astfel indescifrabil.
  - Când destinatarul primește informația criptată, folosește, pentru a o convertii la forma sa originală, o cheie de decriptare numită cheie privată.
  - Cheia privată este secretă și nu va fi niciodată transmisă prin internet.

Protecția în mediul online

- Nu dați informațiile de pe cardul bancar oricui.
  - Există opțiuni pentru efectuarea cumpărăturilor online fără utilizarea cardului.
  - Odată ce faceți clic pe butonul de finalizare a tranzacției, vânzătorul va efectua tranzacția, până la apariția mesajului de finalizare, nu apăsați nici un buton.
- O companie cu domeniu înregistrat care oferă comerț electronic are www înaintea numelui său și pictograma în formă de lacăt (după autentificare).
  - Un site de comerț electronic are o politică de securitate inclusă pe pagină sa de pornire. Citiți această declarație pentru a vedea care sunt condițiile în care puteți să faceți afaceri cu acest furnizor.
- Când navigați pe un site web pentru a achiziționa ceva, verificați că adresa site-ului este scrisă corect și că site-ul este la standardul pe care îl așteptați de la acea companie.
  - Acest lucru vă poate asigura că sunteți pe adevăratul site al acelui vânzător.

Protecția în mediul online

- **Phishing**
  - *Phishing* (înșelăciune): procesul de obținere a informațiilor personale ale cuiva cu intenția de a comite o infracțiune.
  - Se referă la situația în este creat un site web, identic cu site-ul autentic al unei companii sau bănci renumite, cu scopul de a vă determina să vă autentificați în contul dvs. pentru a obține astfel informațiile dvs. personale.
  - Furtul de identitate: colectarea datelor dvs. personale cu scopul de a le folosi ulterior în contexte frauduloase, de exemplu transferuri de bani spre propriile conturi, obținerea accesului la codurile dvs. PIN, crearea de carduri false folosind identitatea dumneavoastră.

Protecția în mediul online

- **În ce măsură pot partaja informații?**
  - Este responsabilitatea utilizatorului să-și folosească bunul simț pentru a decide câte informații dorește să partajeze cu alții.
  - Extindeți-vă precauțiile din viața reală și în mediul online.
  - Aveți grijă cui acordați încredere în mediul online.
  - Nu partajați și nu faceți schimb de informații personale cu cei cu care conversați în mediul online.
  - Dacă plecați de acasă pentru mai mult timp, nu postați acest lucru pe site-urile rețelelor sociale sau în programele de discuții online.
  - Gândiți-vă bine înainte de a posta fotografii sau texte pe site-urile rețelelor sociale.

Protecția în mediul online

- **Protejarea vieții private**
  - Încălcarea vieții private intervine atunci când informațiile dvs. personale sunt împărtășite cu sau vândute altora fără acceptul dvs.
  - De câte ori vizitați un site web, rămân anumite informații despre dvs.
    - Nu există viață absolut privată atunci când navigați pe internet.
  - Alții pot să obțină informații despre dvs. când vizitați site-uri web.
    - Unele organizații pot înregistra activitatea dvs. când navigați pe site-ul lor.
  - Citiți declarațiile de confidențialitate.
    - Ele specifică în mod clar ce informații urmăresc organizațiile respective și modul în care vor folosi aceste informații.

Protecția în mediul online

- **Sfaturi pentru protejarea vieții private**:
  - Nu completați formulare decât dacă doriți ceva de pe site-ul respectiv.
  - Dacă vă înregistrați pe un site web, asigurați-vă că nu aveți selectată vreo opțiune prin care agreați să primiți e-mailuri de la terți.
  - Ștergeți istoricul site-urilor vizitate.
  - „*Navigarea peste umăr*” (*shoulder surfing*) este o practică de a obține informații personale privind peste umărul unei persoane.
  - Achiziționați software de la companii specializate în servicii de siguranța online și protejarea vieții private.
  - Nu instalați nici un fel de add-in-uri sau bare de instrumente disponibile „la pachet” atunci când descărcați un program.

Protecția în mediul online

- Cea mai simplă regulă când navigați în internet, este bunul simț!
- Există multe surse pe internet care aduc în discuție și explică în detaliu problemele legate de viața privată și oferă sugestii de protecție în mediul online.
- Există o serie de inițiative pentru a împiedica obținerea informațiilor personale sau de contact ale dumneavoastră.
  - Instrumentul „Opt-out” creat de către **N**etwork **A**dvertising **I**nitiative va scana computerul dvs. pentru a identifica toate companiile membre care au plasat fișiere cookie pe acesta cu scopul de a vă oferi reclame personalizate.

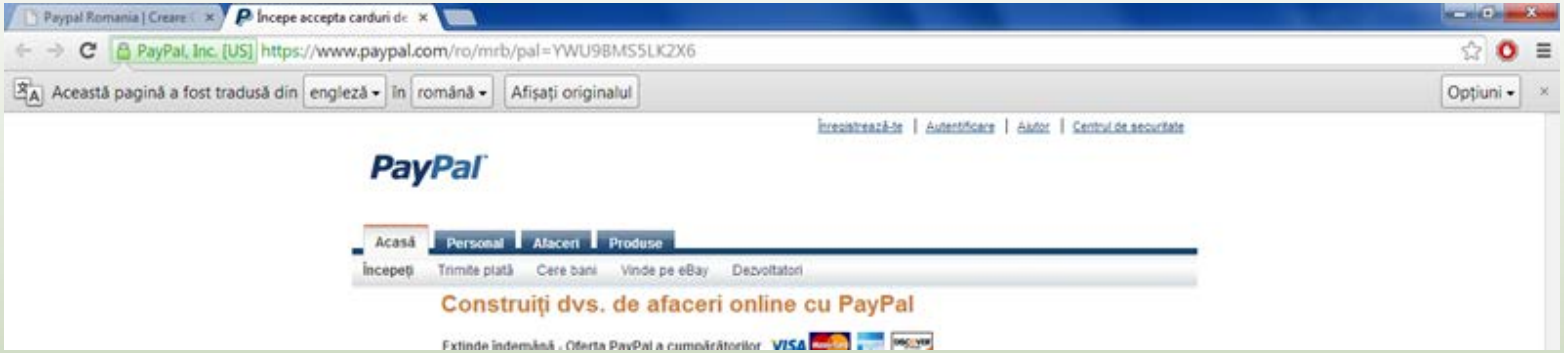
Exercițiu 3 - 1

În cadrul acestui exercițiu, veți explora moduri în care vă puteți proteja pe dvs. și fișierele dvs. de date de pe computer. Pentru a obține un beneficiu maxim în urma acestui exercițiu, trebuie să folosiți Google Chrome și facilitatea sa de traducere automată. Capturile de ecran existente în acest exercițiu sunt din Google Chrome.

1. Într-un browser web, accesați www.paypal-romania.ro. PayPal este o companie internațională de comerț electronic care vă permite să faceți plăți și transferuri de bani prin intermediul internetului. PayPal este folosit în proporții mari în Europa de vest și în S.U.A., cu mai mult de 230 de milioane de conturi. Nu veți crea un cont de PayPal, ci vă veți uita doar la certificatul lor de securitate și veți verifica politica lor de confidențialitate.

Exercițiu 3 - 2

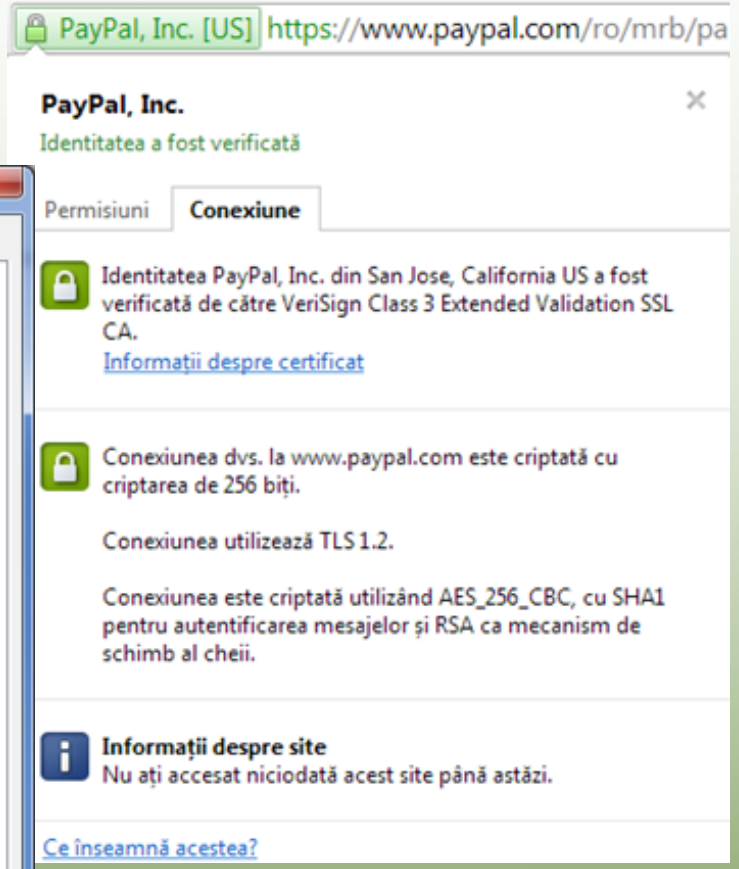
2. Faceți clic pe pictogramă ca și cum ați dori să începeți procesul de înregistrare a unui cont nou.

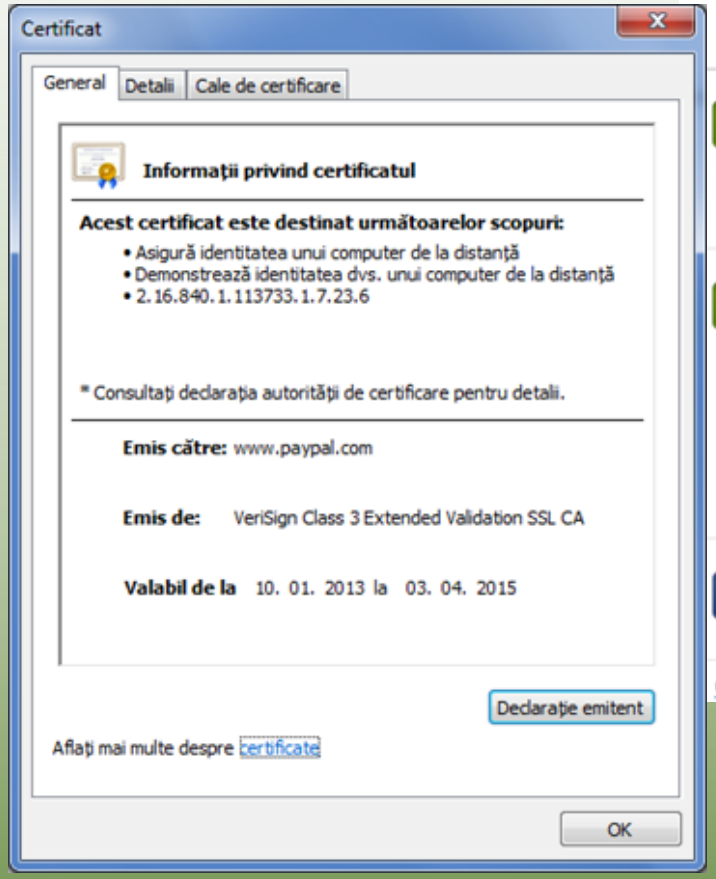


Observați că se deschide o nouă filă de navigare în browserul web. Adresa web conține acum prefixul https, ceea ce înseamnă că ați fost mutat într o zonă securizată a site-ului PayPal. Pictograma reprezentând un lacăt este acum disponibilă pentru a vizualiza mai multe informații despre securitatea acestui site.

Exercițiu 3 - 3

3. Faceți clic pe pictograma lacăt și apoi pe fila Conexiune.
4. Citiți detaliile de pe fila Conexiune și apoi faceți clic pe linkul Informații despre certificat.





Fila **General** arată că certificatul a fost emis de VeriSign pentru www.paypal.com.

Exercițiu 3 - 4

5. Faceți click pe **OK** pentru a închide caseta de dialog Certificat.
6. Derulați în josul paginii și faceți clic pe linkul **De confidențialitate**.
7. Citiți primele câteva paragrafe pentru a vedea ce face PayPal cu informațiile pe care le oferiți când vă înregistrați pe site.
8. În bara de adresa, tastați `www.apple.com` și apăsați **Enter**.

   Observați că această pagină nu are nici un fel de securitate fiind prima pagină a site-ului Apple, destinată doar informării utilizatorilor asupra produselor și serviciilor pe care le oferă compania.
9. Faceți clic pe **iTunes** din meniul aflat în antetul pagini.

   Apple încă nu afișează pictograma lacăt pentru a indica o zonă securizată deși puteți descărca software ul de pe această pagină. Acest lucru se întâmplă pentru că iTunes este un produs asupra căruia, deși Apple are drepturi de autor, este disponibil gratuit pentru oricine prin intermediul unei licențe de tip Creative Commons.

Exercițiu 3 - 5

10. Derulați în josul paginii și faceți clic pe linkul denumit **Politica de confidențialitate**.
11. Citiți politica de confidențialitate de aici pentru a vedea cum Apple se raportează la informațiile pe care le-ar putea obține din orice tip de achiziție sau înregistrare.
12. În bara de adrese, tastați: `http://computer.howstuffworks.com/internet/social- networking/information/10-things-you-should-not-share on-social-networks.html` și faceți clic pe **Enter**.
13. Folosiți butoanele **Prev** și **Next** pentru a citi care sunt cele 10 lucruri pe care nu este recomandabil să le partajați pe rețelele sociale.

    Remarcați că deși acest articol a fost scris în 2009 el se aplică și rețelelor de sociale actuale. Încă odată: cantitatea de informație pe care alegeți să o distribuiți rămâne la latitudinea dvs., dar luați în considerare felul în care unele din informații vă pot afecta viața sau pe cea a prietenilor sau a familiei dvs.

Exercițiu 3 - 6

14. În bara de adresă, tastați `www.google.com` și faceți clic pe **Enter**.
15. În câmpul de căutare tastați: `risks of buying online` sau `riscurile achizițiilor online` și faceți clic pe **Enter**.
16. Uitați-vă în lista de rezultate și apoi faceți clic pe unul dintre linkurile care prezintă interes pentru dvs., cum ar fi un articol care vă dă sfaturi despre cum să faceți achiziții online.
17. Închideți fereastra de navigare când ați terminat.

Sumarul lecției

- Standardele pentru comunicarea profesională
- Cum să evitați comportamentul inadecvat în mediul online
- Proprietatea intelectuală, dreptul de autor și licențierea
- Noțiuni de ergonomie și amenajarea spațiului de lucru
- Protejarea computerului împotriva amenințărilor software
- Ce sunt virușii și cum să evitați infectarea computerului
- Protejarea activităților de comerț electronic

Întrebări recapitulative

1. Când trimiteți un email unui potențial angajator, ce stil de scriere ar trebui să folosiți pentru scrisoarea de intenție și pentru CV?
   a. Formal și profesional
   b. Uzual
   c. O combinație între a și ceva umor de business
   d. Combinație între a și b.

2. Ați scris o lucrare de cercetare excepțională pe tema condițiilor economice în 2010. Un profesor citește acum o altă lucrare cu fragmente identice existente și în lucrarea dumneavoastră. Acesta este un caz de…?
   a. Încălcare a dreptului de autor
   b. Utilizare rezonabilă (fair use)
   c. Plagiat
   d. Creative commons

Întrebări recapitulative

3. Care sunt diferențele între cele două forme de calomniere *libel* și *slander*?
   a. Libel se aplică numai în cazul celebrităților.
   b. Slander este forma orală a calomniei, pe când libel este forma scrisă a acesteia.
   c. Amenda pentru slander este mai mare.
   c. Nu există nici o diferență.
   d. a și c.

4. Când alegi o parolă securizată, aceasta ar trebui să:
   a. Aibă maximum 8 caractere.
   b. Fie o combinație de majuscule și minuscule.
   c. Folosească toate cifrele.
   d. Conțină cel puțin un simbol.
   e. Aibă minimum 8 caractere.
   f. Toate cele de mai sus.
   g. b, d și e.

Întrebări recapitulative

5. Ce sunt fișierele reziduale?
   a. Fișiere care rămân pe computer întotdeauna.
   b. Fișiere ale SO care vă ajută să instalați imprimanta sau alt dispozitiv.
   c. Fișiere care identifică și validează id-ul și parola dvs. de rețea.
   d. Fișiere rămase pe un dispozitiv de stocare după dezinstalarea unui program.

6. După actualizarea unui program anti-virus ce ar trebui să faceți?
   a. Cereți ajutorul administratorului de rețea.
   b. Instalați fișierul descărcat.
   c. Scanați computerul pentru a vă asigura că nu are viruși, spyware sau adware.
   d. Este nevoie doar de repornirea computerului.

Întrebări recapitulative

7. Pentru a preveni RSI puteți lua următoarele măsuri?
   a. Stați pe un scaun ce oferă sprijin lombar și cotiere.
   b. Folosiți o tastatură ergonomică.
   c. Ajustați înclinarea monitorului.
   d. Folosiți un suport căptușit pentru odihna mâinilor în perioadele în care nu tastați.
   e. Stați pe un scaun care are posibilitatea de ajustare a înălțimii.
   f. Toate cele de mai sus.

Întrebări recapitulative

8. Care dintre următoarele recomandări au rolul de a vă proteja confidențialitatea în mediul online?
   a. Nu completați niciun formular dacă nu sunteți interesat de informațiile pe care le oferă compania în cauză.
   b. Folosiți un pseudonim în cadrul unor forumuri publice sau bloguri.
   c. Nu bifați opțiunea de a primi informații de la parteneri ai companiei.
   d. Toate cele de mai sus.
   e. a și b