Informație și comunicare

Lecția 1

INTERNETUL

1.1. Termeni şi concepte
1.1.1. Înțelegerea și diferențierea termenilor Internet și World Wide Web (www)

- Internetul este o reţea globală de calculatoare interconectate, care permite comunicarea între milioane de utilizatori din întreaga lume.
- Reţeaua Internet a fost creată iniţial ca o uriaşă bază de date pentru a fi utilizată în scop ştiinţific şi educaţional. În acest sens, rolul predominant al reţelei internet era cel de documentare şi de comunicare.
- Ulterior, datorită creşterii numărului de calculatoare conectate la Internet, a crescut şi numărul de site-uri ale diferitelor organizaţii care oferă conţinut informaţional, şi implicit numărul de vizitatori ai acestor site-uri, posibili consumatori de produse sau servicii.

Cele mai importante servicii oferite de Internet sunt:

- ***World Wide Web (WWW) -*** reprezintă un sistem de documente şi informaţii legate între ele, accesate prin Internet. Cu ajutorul unui browser Web (Internet Explorer, Mozilla Firefox, Google Chrome, etc) utilizatorul are acces la informaţii de tip text, audio, video, etc. Documentul de bază al WWW este pagina Web.
- ***E-mail (poştă electronică)*** - trimiterea şi primirea de mesaje în format electronic pe internet;
- ***Mesagerie instantanee (instant messaging)*** - conversaţie în timp real pe Internet între două sau mai multe persoane;
- ***VOiP (Voice over Internet IP)*** - servicii de telefonie prin Internet;
- ***RSS (Really Simple Syndication)*** - distribuţia ştirilor şi articolelor publicate pe internet.
- ***FTP (File Transfer Protocol)*** - transfer rapid de fişiere;
- ***Newsgroups*** - colecţii cu informaţii globale actualizate frecvent, organizate mai mult sau mai puţin în jurul unui anumit subiect cu relevanţă publică;
- ***Comunităţi online*** - serviciu disponibil pe Internet, creat cu principalul scop de a conecta utilizatori cu aceleaşi interese, activităţi, hobby-uri.

1.1.2. Definirea termenilor: URL, hyperlink, ISP

Uniform Resource Locator (URL) este o adresă de localizare şi identificare a unei resurse existente pe Internet.

Un URL este format din două părţi:

- numele protocolului
- Numele domeniului.
- ***Un protocol*** este o metodă prin care datele sunt transmise de ta un calculator la altul prin intermediul Internetului.

Cele mai importante protocoale sunt:

Hypertext Transfer Protocol (HTTP) este metoda cea mai des utilizată pentru accesarea informaţiilor în Internet, informaţii păstrate pe servere World Wide Web (WWW).

Hypertext Transfer Protocol Secure (HTTPS) este un protocol de comunicaţie destinat transferului de informaţie criptată prin intermediul WWW. HTTPS este în acelaşi timp o metodă de autentificare a server-ului web care îl foloseşte, prin intermediul aşa-numitelor **certificate digitale**, emise de o autoritate de certificare (de exemplu VeriSign). Se pot consulta informaţii despre identitatea server-ului prin click pe butonul cu un lacăt ce apare în bara de adrese sau de stare a browser-ului utilizat.

Conexiunile HTTPS protejează de intruşi transferul datelor şi sunt folosite în mare parte în operaţiuni de plată pe Internet şi operaţiuni importante în cadrul sistemelor informaţionale corporative.

File Transfer Protocol (FTP) este un protocol (set de reguli) utilizat pentru accesul la fişiere aflate pe servere din reţele de calculatoare particulare sau din Internet.

- *Un nume de domeniu* reprezintă o adresă unică care identifică locaţia unui site Web. Cele maî cunoscute domenii sunt cele:
  - **generice** - indică în general un domeniu organizaţional şi este de obicei format din 3 litere

com	Organizaţii şi societăţi comerciale
edu	Instituţii educaţionale
gov	Organizații guvernamentale
int	Organizaţii internaţionale
mil	Organizaţii militare
net	Centre de administrare a reţelelor mari
org	Organizații non - profit

- **de țară** - reprezintă un cod cu ajutorul căruia se identifică ţara de apartenență a domeniului și este de obicei format din 2 litere.

au	Australia
ca	Canada
ch	Elveţia
de	Germania
fr	Franța
it	Italia
pi	Polonia
ro	Romania
ru	Rusia
uk	Marea Britanie

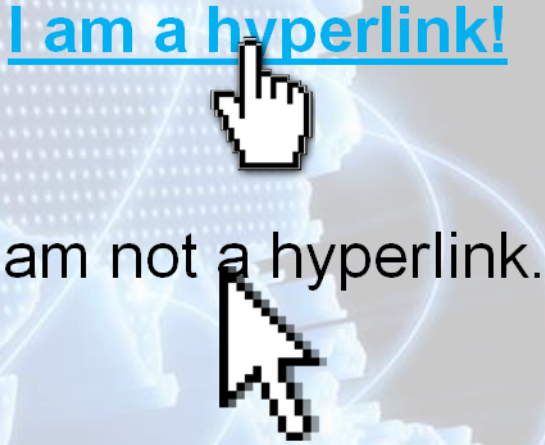
Astfel, în cazul adresei http://www.euroaptitudini.ro

- *http* reprezintă numele protocolului

- www.euroaptitudini.ro reprezintă numele domeniului

Numele domeniului constă în mai multe părţi, separate prin punct.

- Domeniul cel mai din dreapta reprezintă nivelul cel mai înalt (în cazul nostru ro}
- Următorul nivel spre stânga reprezintă subdomeniul (în cazul nostru euroaptitudini)
- Ultimul nivel spre stânga reprezintă subdomeniul de nivel inferior (în cazul nostru www)

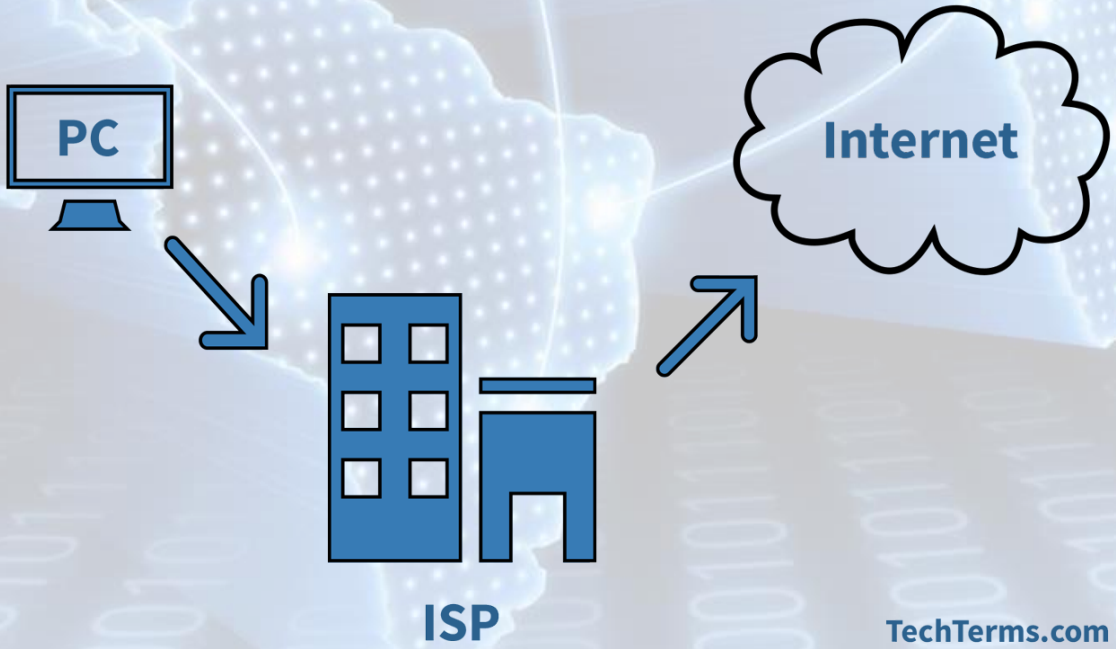


- Un **hyperlink** (folosit mai des sub numele de **link)** reprezintă un cuvânt, grup de cuvinte sau imagine care, în momentul accesării, realizează o legătură către alte părţi ale aceluiaşi document, alte documente sau secţiuni din alte documente.
- Pentru accesarea unui link, pur şi simplu se execută click stânga mouse pe linkul respectiv.

Accesarea unui link poate determina următoarele acţiuni:

- salt la o altă parte a aceleiaşi pagini;
- salt la o altă pagină a aceluiaşi website;
- salt la o altă pagină web;
- permisiunea de a descărca un fişier;
- lansarea unei aplicaţii, unui fişier video sau audio

- **ISP (Internet Service Provider)** este denumirea generică dată unei firme care oferă acces la Internet şi servicii conexe.



1.1.3. Ce este un browser web şi pentru ce este el folosit

- **Un BROWSER WEB** reprezintă o aplicaţie care ne permite să comunicăm şi să afişăm pe monitor text, grafică, video, muzică şi alte informaţii localizate pe o pagină Web.
- Dintre cele mai cunoscute browsere web enumerăm: Internet Explorer, Opera, Mozilla Firefox, Google Chrome.

1.1.4. Ce este un motor de căutare şi pentru ce este el folosit

- **Motorul de căutare** este un program disponibil pe Internet cu ajutorul căruia se pot căuta diferite informaţii. Această căutare se realizează după un anumit cuvânt sau o anumită combinaţie de cuvinte, având ca rezultat afişarea adreselor web a paginilor ce conţin cuvântul respectiv.
- Exemple de motoare de căutare: **Google, Yahoo, Bing etc.**

1.1.5. Înţelegerea termenilor RSS (Really Simple Syndication) şi podcast

- **RSS (Really Simple Syndication)** este o metodă folosită pentru distribuţia ştirilor şi articolelor publicate pe Internet.
- RSS oferă conţinut web sau sumaruri de conţinuturi web, împreună cu legături către conţinutul complet al respectivei surse de informaţii.
- RSS oferă această informaţie sub forma unui fişier numit „feed" sau ”canal”.
- În plus, feed-urile web permit cititorilor fideli anumitor pagini să fie informaţi la actualizarea conţinutului de pe aceste pagini web, prin folosirea unui soft special (numit client RSS).
- Exemple de clienţi RSS: Google Reader, FeedDemon, NewzCrawier, etc. Aceste programe oferă instrumente de actualizare automată, gestiune, sincronizare şi etichetare a conţinutului RSS.
- în paginile web, feed-urile RSS sunt de obicei legate de cuvântul "Subscribe" ("Subscrie"), un pătrat portocaliu,  sau de literele XML sau RSS

Podcast este o metodă de distribuție a fișierelor în format multimedia (de obicei fișiere audio și video). Fișierele pot fi descărcate şi redate pe echipamente mobile sau calculatoare ce acceptă formatul în care acestea au fost create.

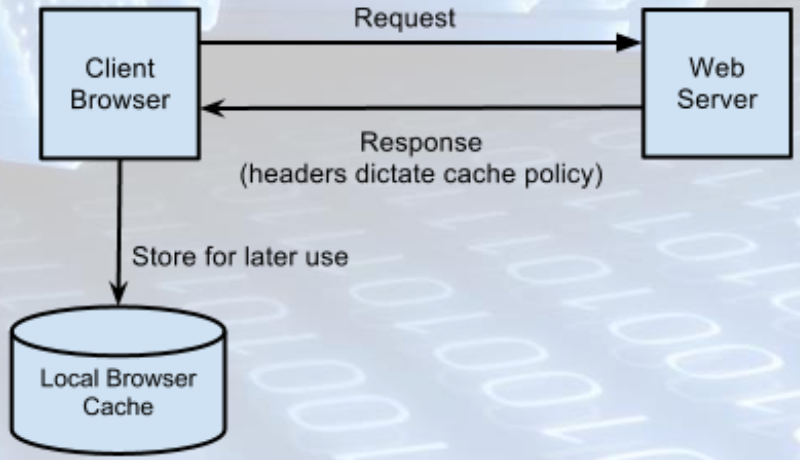
Siturile de podcasting pot oferi fişierele spre descărcare şi ascultare off- line sau pentru redare directă on-line. Metoda de bază este totuşi aceea de descărcare prin intermediul unui cititor de conţinut RSS.

Termenul „podcast" este o combinaţie a cuvintelor „iPod" şi „cast" (difuzare). Multe site-uri, pe baza unui abonament, vă permit să descărcaţi manual conţinut podcast şi pot fi identificate printr-o imagine asemănătoare cu cea de RSS la care se adaugă o pereche de căşti. Dacă doriţi ca acest conţinut sa fie actualizat si descărcat automat, atunci folosiţi un program (client) de podcasting.

Exemple de clienţi podcast: HappyFish, Doppler, iTunes, etc.

1.1.6. Înţelegerea termenilor cookie & cache

- **Cookie** reprezintă informaţii pe care un site web le păstrează pe hard disk-ul calculatorului referitor la opţiunile şi particularităţile utilizatorului, astfel încât, la o a doua vizitare a site-ului respectiv, particularităţile să fie încărcate automat.
- Cookie-urile sunt folosite pentru autentificare, precum şi pentru urmărirea comportamentului utilizatorilor şi reţinerea preferinţelor acestora.
- **Internet Browser Cache** reprezintă locui unde se păstrează temporar copii ale ultimelor pagini vizitate. Motivul este că, în cazul unei vizitări ulterioare a aceluiaşi website, informaţiile sunt rapid încărcate de pe harddisk, accesul fiind mult mai rapid decât la cel de pe Internet.



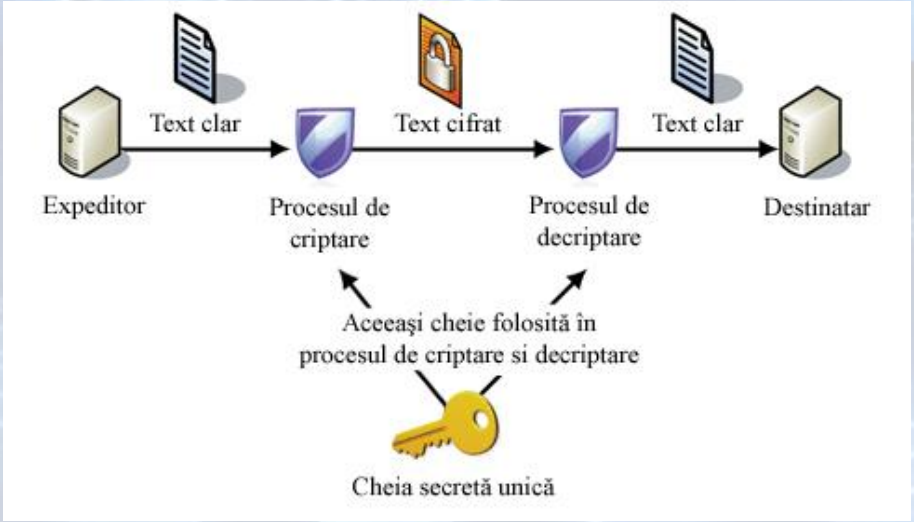
1.2. Securitate

1.2.1. Conceptul de site web protejat

- Un site web protejat reprezintă un site la care accesul se face restrictiv, pe baza unui nume de utilizator (username) şi a unei parole (password).
- De asemenea, un site web protejat este identificat prin textul **https** în cadrul adresei sale şi prin semnul unui lacăt afişat în bara de adrese sau în cea de stare.
- Cel mai des întâlnit exemplu este orice site de mail.

1.2.2. Înţelegerea termenului de criptare a datelor

- Criptarea sau codificarea datelor este **procesul de ascundere a informaţiei pentru a o face ilizibilă**.
- **Scopul** criptării este acela de a nu permite persoanelor neautorizate accesul la anumite date în timpul transmiterii lor sau atunci când sunt păstrate pe diverse suporturi de stocare. Pentru decodificarea datelor, este necesară o cheie de decodificare.

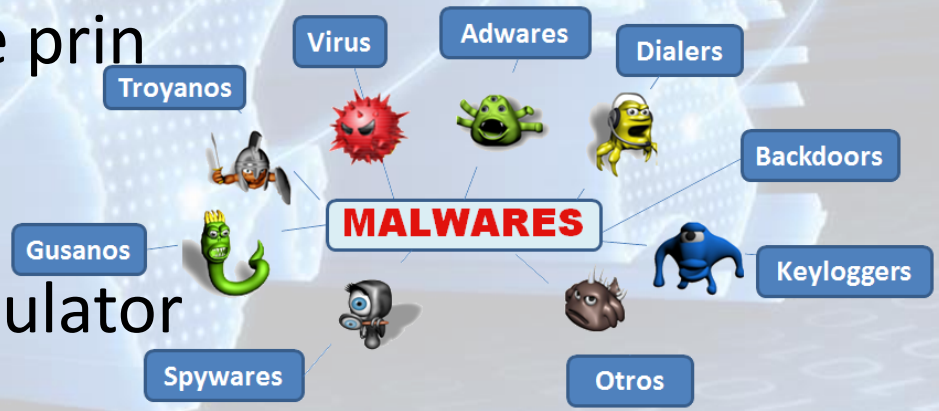


1.2.3. Conceptul de certificat digital

- Certificatul digital reprezintă un **instrument în stabilirea unui canal securizat** pentru comunicarea informaţiilor confidenţiale. Certificatul digital este utilizat pentru o gamă variată de tranzacţii electronice ce include: e-mail, comerţ electronic, transfer electronic de fonduri.
- Certificatul digital este o semnătură electronică ce îmbracă două forme:
  - fie certificatul identifică expeditorul unui document
  - fie certificatul dovedeşte autenticitatea unui site Web către utilizatorii săi.
- În cazul primei forme, semnătura digitală este creată prin criptarea conţinutului documentului, folosind cheia criptografică a expeditorului. Aceasta face ca semnătura să fie unică. Orice modificări aduse documentului afectează semnătura, oferindu-se astfel integritate. Certificatele sunt emise de autorităţi de certificare, care îşi asumă responsabilitatea pentru identificarea utilizatorilor şi pentru acordarea cheilor.
- În cazul celei de a doua forme, certificatul se bazează pe recunoaşterea sa de către autoritatea de certificare.

1.2.4. Termenul de malware. Tipuri de viruşi

- Odată cu apariţia calculatoarelor şi, ulterior, a reţelelor de calculatoare au început să apară şi să se răspândească şi viruşii informatici, producând pagube însemnate prin compromiterea datelor stocate pe computerele oamenilor obişnuiţi sau ale instituţiilor.
- *Viruşii informatici* sunt microprograme pentru calculator create cu scopul declarat de a distruge datele sau echipamentele hardware ale calculatorului. Viruşii au proprietatea de a se extinde şi duc la funcţionarea necorespunzătoare a sistemului de operare şi aplicaţiilor.



Virusul informatic este definit ca un software cu două **caracteristici** principale:

• Se auto-execută. Virusul se poate ataşa altor programe sau se poate ascunde în codul care rulează automat la deschiderea anumitor tipuri de fişiere.

• Se auto-multiplică. Acest lucru este posibil prin ataşarea virusului la alte programe din computer sau prin suprascrierea acestora. Virusul se autorăspândeşte cu ajutorul dispozitivelor de stocare sau a oricărei alte forme de schimb de date, nu numai în sistemul de calcul, dar şi în întreaga reţea.

Viruşii se **clasifică** în:

- Viruşi Hardware: afectează hard discul sau memoria
- Viruşi Software: afectează fişierele şi programele aflate în memorie sau pe disc, inclusiv sistemul de operare sau componente ale acestuia.

Câteva dintre **efectele** pe care le generează viruşii software sunt:

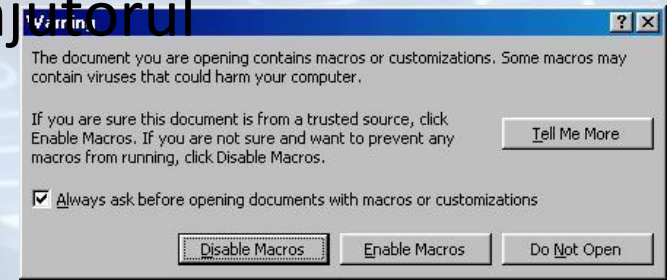
- distrugerea unor fişiere;
- modificarea dimensiunii fişierelor;
- ştergerea totală a informaţiilor de pe disc, inclusiv formatarea acestuia;
- distrugerea tabelei de alocare a fişierelor, care duce la imposibilitatea citirii informaţiei de pe disc;
- diverse efecte grafice/sonore inofensive;
- încetinirea vitezei de lucru a calculatorului până la blocarea acestuia.

- Viruşii se pot clasifica în funcţie de efectele lor şi modul în care acţionează. Printre cei mai importanţi, amintim:
  - *vierme (worm)* - foloseşte o reţea de calculatoare pentru a se reproduce de la un calculator la altul şi poate realiza această acţiune fără nici o intervenţie din partea utilizatorului. Acest lucru se datorează deficienţelor de securitate de pe computerul ţintă. Spre deosebire de un virus de calculator, nu are nevoie să se ataşeze de un program existent. Obiectivul principal constă în blocarea calculatoarelor şi reţelelor. Spre deosebire de viruşi, viermii nu infectează fişierele.
  - *cal troian* - este un program software rău intenţionat, care se ascunde în interiorul altor programe. El intră în computer ascunzându-se în interiorul unui program legitim, cum ar fi un economizor de ecran (screen saver). Apoi, introduce un cod în sistemul de operare, care permite accesul şi controlul deplin la calculatorul infectat. La instalare, nu creează suspiciuni utilizatorului şi nici nu atrage atenţia. Acest tip de virus atacă şi distruge datele de pe hard-disk.

  - *programe spion (spyware)* - aplicaţii ce colectează informaţii despre o persoană sau organizaţie fără ştiinţa şi consimţământul acestora. Aceste programe fură date ce sunt folosite în scopuri publicitare sau financiare. Tipul de informaţii furate variază de la nume şi parole de utilizatori, adrese IP şi DNS până ta date utilizate în operaţiuni de plată folosind servicii de online banking şi magazine virtuale.

- *virus* - sunt programe de calculator proiectate să infecteze fişiere. Se găsesc în codurile programelor infectate şi acţionează când aceste programe sunt rulate. Pot fi programaţi să se activeze când sunt îndeplinite anumite condiţii (o anumită dată calendaristică, o anumită acţiune a utilizatorului, etc). Aceste mici programe distrug informaţiile aflate pe calculator şi împiedică funcţionarea aplicaţiilor.
- *păcăleli (hoax)* - sunt mesaje trimise prin e-mail care conţin avertizări false despre un virus existent şi care cer să fie avertizate toate persoanele cunoscute. Uneori, aceste avertizări conţin şi fişiere ataşate menite, chipurile, să stopeze sau să elimine virusul. Retrimiterea mesajului la alţi destinatari determină multiplicarea virusului.

- *macro* - se va folosi de funcţionalitățile Visual Basic for Applications (VBA) de a crea macrocomenzi oferite de unele programe cum ar fi Microsoft Office. Dacă utilizatorul va folosi facilităţile oferite prin crearea de comenzi macro pentru automatizarea anumitor activităţi, virusul va folosi această facilitate pentru a se răspândi şi a-şi îndeplini scopul distructiv. Viruşii de macro infectează fişierele de tip document şi se răspândesc cu ajutorul documentelor transmise între utilizatori.



1.2.5. Modalităţi de transmitere a viruşilor

- Viruşii pot pătrunde în calculator:
  - prin intermediul programelor, documentelor şi imaginilor descărcate de pe Internet (operaţie denumită *download),*
  - prin intermediul fişierelor ataşate primite prin e-mail,
  - prin intermediul dispozitivelor de stocare.
- De aceea este recomandat ca la folosirea uneia din aceste căi să se ruleze un program antivirus.
- Programele antivirus sunt programe create special pentru a efectua următoarele operaţiuni:
  - să detecteze viruşii prin verificarea conţinutului fişierelor şi semnalarea prezenţei semnăturii unui virus cunoscut sau a unor secvenţe suspecte în interiorul lor
  - să dezinfecteze sau să şteargă fişierele infestate de viruşi cunoscuţi
  - să prevină infectarea prin supravegherea acţiunilor din memorie şi semnalarea
  - întâlnirii unor anumite acţiuni ce ar putea fi generate de existenţa în memorie a unui virus
- Există două feluri de antiviruşi după modul în care acţionează:
  - Programe care după ce au fost lansate rămân în memoria calculatorului şi supraveghează fiecare aplicaţie lansată în execuţie.
  - Programe care sunt lansate de către utilizator numai atunci când el doreşte să verifice calculatorul.

1.2.6. Acţiuni împotriva viruşilor

- Pentru a evita anumiţi viruşi sau pentru a-i elimina, va trebui:
  - să aveţi instalat un program antivirus cât mai recent, cu ajutorul căruia să puteţi descoperi şi să eliminaţi eventualii viruşi;
  - programul antivirus pe care îl utilizaţi are o bază de date în care sunt înglobate diferitele tipuri de viruşi pe care programul antivirus îi recunoaşte şi îi elimină. Având în vedere că aproape zilnic apar viruşi noi, trebuie să vă actualizaţi periodic baza de date a programului antivirus astfel încât acesta să poată recunoaşte şi elimina toţi viruşii nou apăruţi. Pentru calculatoarele care au conexiune la Internet, actualizarea se realizează automat.
  - să se scaneze toate fişierele cu regularitate;
  - să se scaneze periodic fişierele din calculator şi de pe diverse suporturi de stocare (memory stick-uri, CD-uri, DVD-uri etc.) înainte de a le folosi;
  - să se scaneze fişierele ataşate primite pe mail;
  - să nu se ruleze programe dacă nu li se cunoaşte proveniența;
  - să se folosească funcţia „macro disable" (dezactivare macrocomenzi), disponibilă în cele mai moderne aplicaţii.

1.2.7. Securitatea informaţiei

- În lucrul cu date importante, securitatea datelor devine un element cheie. De regulă, prin securitatea informaţiei se înţelege asigurarea confidenţialităţii ei. Printre metodele de protejare a datelor amintim:
  - **Restricţionarea accesului fizic la calculator**;
  - Folosirea unui **nume de utilizator** (username) şi a unei **parole** (password) pentru autentificarea pe un calculator;
  - Adoptarea unei politici de **parolare** corespunzătoare:

  Parolele stabilite trebuie concepute astfel încât să fie foarte greu de descoperit de persoanele neautorizate. Pentru aceasta, se recomandă ca aceste parole să nu conţină date personale ale utilizatorului sau să nu fie parole generate automat de către calculator. Trebuie avut în vedere şi faptul că parolele sunt "case-sensitive", în sensul că se face deosebire între caracterele majuscule şi cele minuscule folosite la scrierea parolei.

  De asemenea, este recomandat ca parolele să fie constituite dintr-o combinaţie de litere, cifre şi simboluri, să aibă o lungime corespunzătoare, să fie modificate la un anumit interval de timp şi, cei mai important, să nu fie comunicate altor persoane.

- **Stabilirea drepturilor** pe care le are fiecare utilizator;

  0 modalitate foarte bună de protejare a datelor este crearea utilizatorilor cu diferite drepturi în funcţie de locul pe care îi ocupă aceştia în structura organizatorică a firmei. Astfel, se recomandă accesul restrictiv la date al angajaţilor de pe o treaptă inferioară şi un acces mai puţin restrictiv utilizatorilor de pe un nivel superior.

- **Realizarea de back-up în mod regulat**;

  în tehnologia informaţiei, termenul de backup desemnează realizarea unor copii de siguranţă ale fişierelor din computer pe un dispozitiv extern de stocare hard-disk extern, CD, DVD, memory stick etc.), pentru a putea recupera datele în cazul defectării sistemului. Este recomandabil ca aceste copii de siguranţă să fie păstrate într-o locaţie externă, diferită, de cea în care se află calculatorul ce conţine datele iniţiale.

- **Criptarea fişierelor**

  Criptarea sau codificarea datelor este procesul de ascundere a informaţiei pentru a o face ilizibilă. Scopul criptării este acela de a nu permite persoanelor neautorizate accesul la anumite date în timpul transmiterii lor sau atunci când sunt păstrate pe diverse suporturi de stocare. Pentru decodificarea datelor, este necesară o cheie de decodificare.

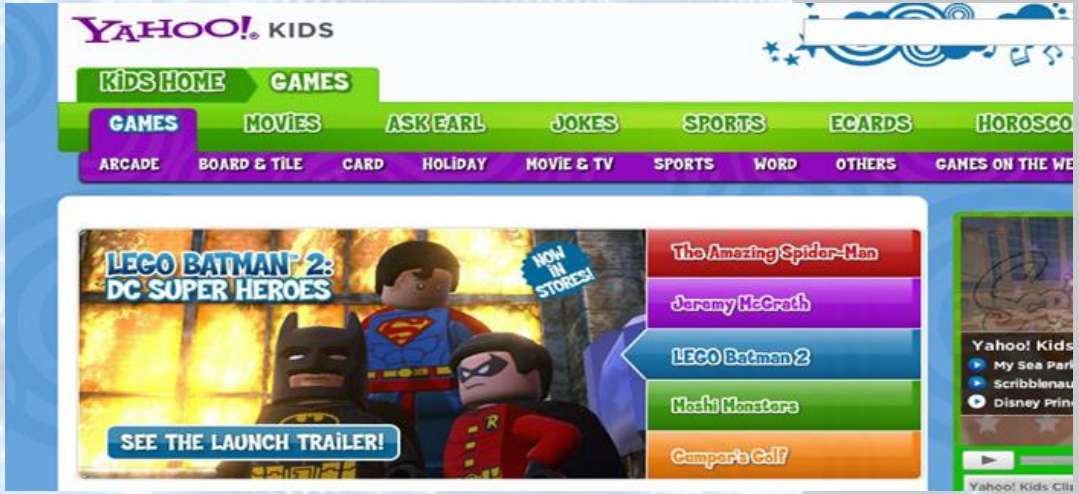
- **Folosirea programelor anti-virus**;

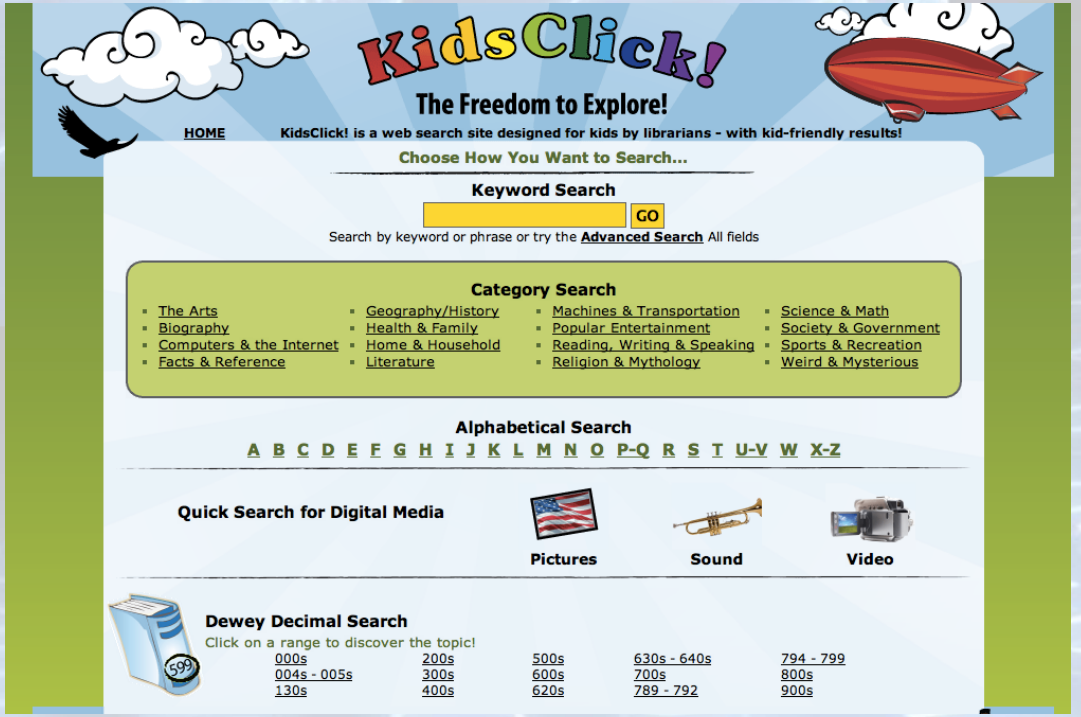
  Folosirea programelor de securitate de tip firewall. Acesta reprezintă un sistem de securitate format dintr-o combinaţie de hardware şi software, destinat protejării unei reţele împotriva accesului neautorizat. El va monitoriza şi filtra în permanenţă transmisiile de date realizate între calculator, reţeaua locală şi Internet.

- **Proxy server-ul** *este o componentă a unui firewall care filtrează informaţiile şi organizează traficul între Internet şi reţele. Prin el, se oferă acces la reţea şi se filtrează diferitele cereri venite din partea utilizatorilor, pentru a evita accesul persoanelor neautorizate. Accesul la o reţea se realizează pe baza unui nume de utilizator şi a unei parole*.

1.2.8. Navigarea sigură pe Internet

- Copiii de azi trăiesc într-o lume bizară şi plină de pericole pe care le implică mediul virtual. Principalele riscuri la care se expun copiii sunt:
- **A fi expuși la conţinut**
  - de aceea se recomandă folosirea filtrelor de căutare ce elimină conţinutul explicit din motoarele folosite.
  - O altă opţiune este folosirea motoare speciale pentru copii cum este Yahoo!Kids şi www.KidsClick.org sau browsere pentru copii cum sunt sunt KidRocket sau SurfKnight.
  - Crearea unei liste de site-uri favorite împreună, pentru a elimina din căutările pe care trebuie să le facă.
- Există lucruri online care sunt nepotrivite pentru copii. Dacă vreodată descoperiți ceva ce pare ciudat sau care vă face să vă simțiți inconfortabil, trebuie să închideți site-ul şi să informați un adult.





- Principalele riscuri la care se expun copiii sunt:
  - **A face publică informaţia personală** - *Internetul poate părea abstract pentru un copil, aşa că este greu să înţelegeți că a face publică informaţia este o problemă gravă. În plus, vă aflați la o vârstă la care mărturisirile sunt un mod de a crea legături cu prietenii. A păstra secrete parola şi alte informaţii personale, este la fel de important ca a închide casa noaptea şi a sta departe de străini.*
  - Un **username** nu trebuie să conţină detalii ce pot duce la identificarea dvs. O **parolă** trebuie să nu fie uşor de ghicit (e o idee bună să includeţi litere sau cifre și caractere speciale).

- Principalele riscuri la care se expun copiii sunt:
  - **A petrece prea mult timp online** – *Trebuie impusă o limită de timp strictă pentru jocurile online. Iar dacă un copil îşi face temele pe calculator, există riscul să fie distras de jocuri sau mesaje instant. Computerul trebuie pus într-un spaţiu public, pentru a putea fi verificat des.*
  - *Adulții trebuie să discute cu copiii despre ceea ce fac pe net.*

- Principalele riscuri la care se expun copiii sunt:
  - **Ştergerea accidentală a fişierelor importante** – de aceea trebuie pregătit un spaţiu virtual sigur înainte de a lăsa copilul la calculator. *Este utilă crearea propriul user, astfel încât să nu poata să şteargă accidental documente importante sau poze de familie (dar asiguraţi-vă că aţi pus parola împreună, astfel încât să o ştiţi şi dumneavostră).*
  - *Instalaţi un antivirus şi un popup blocker - va fi mai puţin probabil să acceseze accidental spyware sau viruşi*.

- Principalele riscuri la care se expun copiii sunt:
  - **Atacurile online** - *Dacă un copil este lăsat să comunice online, este bine să o facă doar cu prieteni adevăraţi din viaţa sa.*
  - *Se pot folosi setările de siguranţă pentru a bloca mesajele de la străini.*

Reguli oniine pe care ar trebui să le urmeze fiecare copil

- Nu oferiți niciodată informaţii personale (nume, vârstă, locaţie, telefon)
- Niciodată nu divulgați parolele
- Nu descărcați jocuri şi programe, chiar dacă sunt gratis, fără permisiunea părinţilor
- Nu deschideți mesaje de la necunoscuţi
- Nu apăsa pe nimic care apare în altă fereastră, chiar dacă arată că un joc e gratis sau îţi oferă o excursie la Disneyland
- Fii mereu politicos şi gândeşte-te înainte de a scrie
- Nu discuta niciodată cu oameni care nu îţi sunt prieteni în viaţa reală

- Programele de Control Parental sunt o soluţie completă pentru protejarea copiilor în timpul utilizării Internetului şi controlul activităţii acestora pe calculator şi Internet. Ele dau posibilitatea să se seteze următoarele opţiuni:
- *Filtrarea şi controlul navigării pe Internet*
  - blochează accesul la anumite site-uri pe baza unei liste predefinite de adrese interzise,
  - analizează conţinutul şi blochează accesul pe anumite pagini pe baza unei liste predefinite de cuvinte interzise
  - permite accesul doar la anumite site-uri pe baza unei liste predefinite de adrese acceptate
- *Controlul utilizării şi accesului pe calculator şi Internet:*
  - limitează timpul petrecut de copii pe calculator şi/sau Internet, prin stabilirea unor intervale orare în care copilul poate avea acces la acestea;
  - limitează tipurile de programe şi fişiere care pot fi descărcate şi instalate pe calculator;
  - blochează accesul la informaţiile personale sau de lucru stocate pe calculator (de exempludocumente, fotografii personale) prin blocarea accesului la anumite fişiere sau partiţii de disc;
  - limitează sau blochează utilizarea unor programe de către copii (messenger, sharing de fişiere, programe utilizate de către părinţi).
  - limitează sau blochează accesul la setările calculatorului.
- *Monitorizarea utilizării calculatorului şi Internetului*
  - întocmeşte lista cu site-urile pe care le-a accesat copilul, astfel că aceasta poate fi verificată de părinţi.
  - întocmeşte rapoarte cu pagini vizitate, programe utilizate, timp alocat, fişiere accesate/create/şterse sau chiar imagini de tip printscreen cu activitatea copiilor pe calculator sau Internet.
  - trimite pe email-ul părinţilor rapoarte periodice cu activitatea copiilor pe calculator.