UTILIZAREA CALCULATORULUI SI A SERVICIILOR ELECTRONICE
GHID PENTRU FUNCTIONARII PUBLICI

Calculatoarele şi Internet-ul au schimbat în mod semnificativ modul în care cetăţenii pot avea acces la serviciile publice. Societatea informaţională este din ce în ce mai prezentă în toate activităţile sectorului public inclusiv prin aplicaţii complexe de e-Government.

Guvernul României promovează diverse proiecte care să facă din serviciile electronice un instrument de reformă a administraţiei publice. Primele rezultate sunt încurajatoare dar arată că această reformă trebuie să aibă loc şi la biroul fiecărui funcţionar public. Ghidul de faţă are ca scop să asigure funcţionarului public câteva cunoştinţe de bază şi bune practici în utilizarea calculatorului şi mai ales a Internet-ului la locul său de muncă. Oferă de asemenea informaţii generale privind diverse proiecte de e-Government din România şi din întreaga lume.

Utilizarea Calculatorului şi a Serviciilor Electronice – Un Ghid pentru Funcţionarii Publici a fost elaborat de către proiectul RITI dot-Gov, în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei.

Proiectul RITI dot-Gov face parte din Iniţiativa pentru tehnologia Informaţiei în România, RITI, a cărei implementare a început în 2002 de către Misiunea din România a Agenţiei Statelor Unite pentru Dezvoltare (USAID), în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. Proiectul RITI dot-Gov este implementat în România de către Internews Network Inc, o organizaţie non-profit cu sediul în Statele Unite ale Americii.

Pentru informaţii suplimentare: www.riti-internews.ro
www.mcti.ro
www.internews.org

Elaborarea cestui ghid a fost posibilă prin asistenţa asigurată de către Centrul Regional de Servicii Budapesta al Agenţiei Statelor Unite pentru Dezvoltare Internaţională, USAID, pentru proiectul RITI dot-GOV, în cadrul Acordului de Cooperare Nr. CA #186-A-00-02-00101-00; LA#GDG-A-00-01-00009-00, implementat de către Internews Network Inc.

Opiniile exprimate în cadrul ghidului aparţin autorului şi nu reflectă în mod necesar vederile Agenţiei Statelor Unite pentru Dezvoltare Internaţională.

1. Administrarea eficientă a resurselor calculatorului

Acest capitol prezintă o serie de concepte, reguli şi sfaturi destinate unei utilizări cât mai eficiente a calculatorului:

- **managementul informaţiilor şi documentelor (fişiere, structurare, legături favorite, arhive, copii de siguranţă, fluxul informaţional);**
- **disciplina (reguli de conduită, punctualitatea, folosirea calculatorului în scopuri personale etc.);**
- **securitatea calculatorului (riscuri, programe utilitare şi sfaturi pentru evitarea riscurilor).**

1.1. Organizarea şi fluxul documentelor

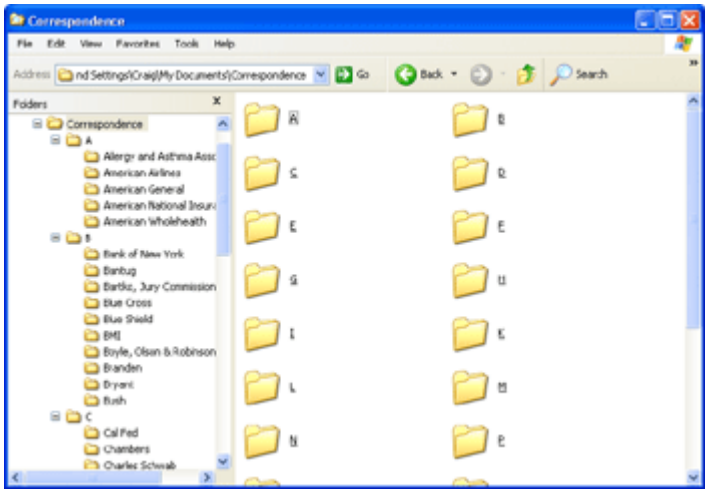
Administrarea documentelor salvate în calculator este similară administrării documentelor pe hârtie – documentele electronice pot fi organizate de asemenea în dosare şi apoi stocate în anumite locaţii. În cazul în care organizarea este deficitară, documentele se pot pierde – la fel ca şi hârtiile.

De aceea este bine să luaţi în considerare următoarele sfaturi, indiferent dacă salvaţi documentele în calculatorul dumneavoastră (pe hard-disk) sau în reţea[1].

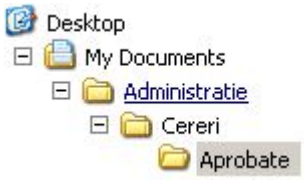
1.1.1. Sfaturi utile

1. Folosiţi un sistem coerent de administrare şi denumire a fişierelor[2]. Astfel veţi găsi uşor documentele de care aveţi nevoie, atunci când aveţi nevoie. Evitaţi structurile prea stufoase – dacă aveţi nevoie să creaţi multe fişiere într-un director şi nu le puteţi vedea pe toate, ordonaţi-le alfabetic.

Salvaţi separat fişierele cu documente şi fişierele cu programe! Astfel evitaţi să ştergeţi din greşeală documente atunci când instalaţi sau actualizaţi programe.



2. Folosiţi denumiri scurte şi concise – care vă ajută la vizualizarea întregii denumiri şi la o navigare mai uşoară în sistemul de fişiere, cum ar fi abrevieri sau denumiri comune. O altă metodă de a regăsi mai repede documentele este introducerea datei în denumire.



[1] Este recomandat ca în fiecare instituţie să existe un set de reguli pentru managementul documentelor. Există numeroase aplicaţii care pot fi utile în acest sens, permiţând stocarea eficientă, organizarea şi regăsirea rapidă a documentelor – aspecte esenţiale pentru orice organizaţie care prelucrează un volum mare de informaţii.

[2] Este indicat să folosiţi denumiri relevante pentru conţinutul dosarelor (folderelor) şi să menţineţi acelaşi sistem de salvare a documentelor pentru a le găsi mai uşor (ex. „Adrese", „Rapoarte", etc.)

3. Separați lucrările în curs de cele terminate. Astfel reduceți numărul de fișiere în care căutați un anumit document, precum şi cantitatea de date pe care să o arhivați. Este util ca lunar să mutați documentele şi fişierele cu care nu mai lucrați în mod curent în altă locație sau să le arhivați.

Fiți selectivi în salvarea fişierelor! Nu salvați documente inutile (de ex. nu toate mesajele e-mail trebuie salvate).

4. Creați „scurtături". Dacă aveți nevoie să accesați acelaşi document din locații/dosare diferite, în loc să creați copii ale aceluiaşi document puteți crea o legătură directă către acesta. Pentru a accesa imediat un anumit dosar puteți crea o legătură directă către acesta pe desktop.

Pentru a găsi un document la care ați lucrat recent puteți folosi directorul de documente recente din meniul start (My Recent Documents).

1.1.2. Distribuirea informațiilor

În lucrul cu documentele, este important să avem mereu în vedere gradul de confidențialitate al a acestora. Astfel, documentele publice trebuie să fie astfel distribuite/publicate încât să devină accesibile tuturor cetățenilor, însă documentele confidențiale trebuie stocate în aşa fel încât să nu poată fi accesate de către persoanele neavizate.

O atenție deosebită trebuie acordată informațiilor confidențiale distribuite în format electronic, întrucât acestea pot fi uşor multiplicate sau distribuite mai departe de către terțe persoane – este de preferat să se precizeze clar şi direct natura confidențială a acestor documente pentru toți destinatarii sau utilizatorii. Mesajele importante pot fi chiar criptate, dacă este cazul, iar documentele pot fi păstrate în foldere sau arhive protejate cu parolă, sau care pot fi accesate doar cu utilizarea unui eToken[3].

1.1.3. Regăsirea informațiilor

Atât în cazul fluxului de documente pe hârtie cât şi în cazul celor electronice, este important să păstrăm referințe despre autorii lor, expeditorii sau destinatarii cărora le-au fost trimise. Astfel, va fi întotdeauna uşor de aflat de unde provin anumite informații sau documente, respectiv cine a fost informat despre anumite schimbări[4].

1.2. Utilizarea calculatorului în scop personal

Calculatorul de serviciu este o resursă a instituției destinată îndeplinirii sarcinilor de serviciu. De aceea este bine ca folosirea acestora în scop personal să situeze în limite decente şi să nu afecteze activitatea desfăşurată în mod curent.

În acest sens este indicat să salvați toate documentele personale (inclusiv e-mail) în foldere separate. Nu abuzați ocupând spațiul de stocare pe hard-disk cu fişiere mari (fotografii, muzică etc.) întrucât există riscul de bloca memoria calculatorului astfel încât programele necesare lucrărilor de serviciu să nu mai poată rula la parametrii optimi.

---

[3] Mic dispozitiv hardware pe care utilizatorul îl poartă asupra sa şi care este necesar pentru accesarea anumitor fişiere/aplicații, asemenea unei parole.

[4] Dacă acest lucru este realizat practic automat în cazul corespondenței transmise prin e-mail, pentru scrisori şi documente este necesar să păstrăm o evidență specială, similară celei a programului e-mail.

Programele instalate pe calculatorul de serviciu sunt supuse prevederilor unor licenţe pentru respectarea cărora instituţia este responsabilă. De aceea nu copiaţi şi nu distribuiţi aceste programe, întrucât este foarte posibil să încălcaţi limitele drepturilor acordate prin licenţă.

Recomandările cu privire la corespondenţa purtată prin e-mail şi cele referitoare la securitate sunt direct aplicabile şi pentru mesajele şi documentele personale. De asemenea, având în vedere faptul că întreaga corespondenţă electronică utilizează acelaşi server, limitaţi-vă numărul mesajelor personale la strictul necesar, pentru a nu suprasolicita reţeaua.

Evitaţi folosirea altor forme de comunicare electronică (cum ar fi chat sau mesagerie instantanee) în scopuri personale, întrucât aceste aplicaţii necesită utilizarea unui volum considerabil din fluxul de date transmise prin reţea.

Nu accesaţi site-uri care pot avea un conţinut ilegal (de ex. programe fără licenţă legală) sau dăunător pentru calculator[5]. Nu vă conectaţi la alte reţele (cum ar fi cele de tip peer-to-peer) decât cele stabilite prin configuraţia reţelei instituţiei.

Este bine să reţineţi că orice mesaje transmise prin Internet neprotejate (adică fără a folosi o metodă de criptare a datelor) sunt comunicaţii nesigure din punctul de vedere al securităţii şi confidenţialităţii. Aşadar respectaţi cu stricteţe politica de confidenţialitate a informaţiilor de serviciu şi nivelul de acces stabilit pentru informaţiile stocate în fişiere şi nu transmiteţi sub nici o formă aceste informaţii persoanelor neautorizate.

Orice operaţiune efectuată pe calculator, indiferent dacă este îndeplinită on-line sau nefiind conectat la Internet, este înregistrată ca „eveniment" într-un jurnal din memoria calculatorului (*computer log*). Mai mult, unele instituţii pot avea instalate programe speciale de monitorizare a utilizării de către un angajat a sistemelor informatice proprii. Aceste programe pot furniza informaţii despre programele accesate, fişierele utilizate, mesajele de poştă electronică trimise şi primite, site-urile de Internet vizitate etc.
De aceea este bine să vă informaţi cu privire la regulamentul de utilizare a calculatorului, pentru a evita efectuarea de operaţiuni neadecvate şi totodată pentru a vă proteja sfera privată a relaţiilor de muncă[6].

1.3. Organizarea e-mail-ului

1.3.1. Gestionarea informaţiei

Tehnologia ajută oamenii să comunice mai uşor, mai repede, în orice loc, dar poate fi în acelaşi timp o sursă de stres datorată avalanşei de informaţii cu care suntem copleşiţi. Dacă primiţi 100 şi trimiteţi 20 de e-mail-uri zilnic, cantitatea de informaţie devine copleşitoare şi pare aproape imposibil să-i faceţi faţă. În plus, o mare parte dintre aceste e-mail-uri sunt neimportante şi cu toate acestea ne răpesc o mare parte din timp, ajungând chiar să pierdem 1-2 ore pe zi doar răspunzând la e-mail-uri. În acest caz, e-mail-ul, în loc să ne ajute, ne opreşte din activităţile importante.

---

[5] În general site-urile cu jocuri (în special cele unde puteţi juca on-line), cu conţinut pentru adulţi, etc. conţin programe-spion sau chiar viruşi. V. pentru detalii secţiunea de securitate a acestui capitol.
[6] V. pentru detalii „Aspecte actuale ale monitorizării angajaţilor la locul de muncă în ceea ce priveşte utilizarea Internet-ului", *Bogdan Manolea* - http://www.legi-internet.ro/monitorizare.htm

Cum putem gestiona e-mail-ul astfel încât să avem timp şi pentru celelalte activităţi zilnice? Un răspuns rapid ar fi: organizarea. Nu lăsaţi e-mail-urile să se adune în Inbox. identificaţi rapid e-mail-urile importante şi decideţi cum trebuiesc procesate.

Organizare şi automatizare

Pentru început, trebuie să sortaţi e-mail-urile pe care le primiţi, astfel încât să le puteţi identifica pe cele importante şi pe cele la care trebuie să răspundeţi.

Inbox - reguli de bază:

1. **În Inbox nu trebuie să se găsească decât e-mail-uri cu adresa dumneavoastră în To:[7] şi CC:.[8]** Dacă numele Dvs. este într-unul din aceste două câmpuri, înseamnă că expeditorul a dorit să citiţi acest mesaj şi poate chiar să răspundeţi (mai ales dacă adresa Dvs. este în câmpul To:).
2. **Mesajele trebuie să fie sortate după priorităţi.**
   În ordine, veţi răspunde la mesajele primite de la:
   - Director, manager sau supervizor
   - Echipele şi proiectele la care lucraţi (trebuie să fiţi la curent cu evoluţia proiectelor şi să răspundeţi în timp util la solicitările colegilor de echipă).
   - Alte persoane.

Suntem tentaţi să citim toate mesajele primite de pe listele de discuţii la care suntem abonaţi şi toate glumele primite de la prieteni. Este indicat să nu pierdeţi timp preţios cu acestea, sau măcar să amânaţi până la sfârşitul zilei când aţi terminat lucrurile importante. Altfel riscaţi să ajungeţi la ora prânzului şi să constataţi că nu aţi terminat de citit e-mail-urile. Din acest motiv, toate mesajele primite care nu corespund regulilor de mai sus nu au ce căuta în Inbox şi astfel nu veţi fi tentaţi să le examinaţi.

Automatizarea sortării mesajelor

Programele de e-mail ne ajută la sortarea mesajelor folosind reguli sau filtre şi, respectiv, diverse variante de vizualizare pentru mesaje.

Reguli/filtre

Trebuie să începeţi prin a crea o ierarhie de foldere pentru mesajele primite. Felul în care construiţi ierarhia depinde de preferinţele fiecăruia. În mod normal se creează un folder pentru fiecare proiect sau grup de persoane cu care corespondaţi şi câte un folder pentru fiecare listă de discuţii (sau grup de liste cu tematică asemănătoare). Se creează de asemenea foldere în care veţi muta mesajele pentru arhivare.

Trebuie create apoi regulile/filtrele pentru procesarea mesajelor. O astfel de regulă are următorul format:

---

[7] To: şi CC: reprezintă câmpurile cu adresa destinatarilor principali (TO) şi respectiv a destinatarilor secundari (CC), cărora li se trimite o copie a mesajului.

[8] Primul lucru care-l vedem când deschidem programul de e-mail este Inbox-ul. Prin natura umană, ochii noştri se vor opri asupra primului mesaj din Inbox. Vom fi tentaţi să-l citim, chiar dacă acesta este unul neimportant. Astfel vom pierde vremea cu mesaje pe care am putea să le citim mai târziu (de exemplu mesajele primite pe liste de distribuţie) sau chiar să le ignorăm.

Dacă <regulă> (ex:e-mail-ul a fost trimis către o anume listă de distribuție)
Atunci mutare în folderul <specificat> (ex: folderul creat pentru respectiva listă de distribuție)
<Excepție> (ex: dacă numele dumneavoastră este în caseta To sau CC).

Vizualizare: culori şi etichete
Pentru a identifica mai rapid ordinea în care trebuie să răspundeți, unele programe de e-mail pot colora automat mesajele în funcție de anumite criterii (spre exemplu, cele primite de la manager cu roşu, mesajele din partea echipei cu albastru etc.). Astfel, puteți observa dintr-o privire dacă aveți în Inbox mesaje importante sau dintr-o anumită categorie.
Mesajelor de poştă electronică li se poate ataşa o etichetă pentru urmărire, pentru a simplifica clasificarea şi găsirea lor ulterioară. Unele programe de e-mail permit chiar vizualizarea doar a unei categorii de e-mail-uri, cum ar fi cele care corespund unei anume etichete, sau cele necitite.

Procesarea e-mail-urilor

După citirea unui e-mail, aveți 4 variante principale de procesare:

Acțiune	Descriere
Răspundeți	Răspundeți la mesaj imediat sau îl lăsați în continuare în Inbox pentru a răspunde mai târziu. După ce ați răspuns, mutați mesajul folderul corespunzător.
Forward	Redirecționați mesajul către alte persoane (dacă nu e problema dumneavoastră sau informațiile îi interesează şi pe ei), după care mutați e-mail-ul din Inbox (la fel ca mai sus).
Salvați în alt director	Salvați mesajul pentru referință ulterioară în alt folder. Puteți crea etichete pentru urmărirea/regăsirea ulterioară a mesajului, iar unele programe de e-mail pot să reamintească de acest mesaj la o anumită dată.
Ştergeți	Ștergeți mesajul, dacă nu este de interes.

Când citiți e-mail-ul?

Acest lucru depinde foarte mult de natura muncii:

- Dacă este critic să răspundeți rapid la toate mesajele (de exemplu lucrați la departamentul de relații cu publicul sau de suport tehnic) atunci probabil că programul de e-mail va rula tot timpul şi va trebui să citiți şi să răspundeți imediat la toate mesajele primite.
- Dacă activitatea dumneavoastră nu presupune răspunsuri imediate atunci, cel mai bine este să rezervați acestei activități o anumită perioadă a zilei (de exemplu la sfârşitul programului sau dimineața).

Căutarea mesajelor

Majoritatea programelor de e-mail actuale oferă facilități de căutare pentru a regăsi mesajele primite sau trimise anterior. Căutarea se poate face după diverse criterii: cuvinte cheie (din tot mesajul sau doar din câmpul de subiect), dată, importanță, folosind etichetele (vezi mai sus) etc.

Foldere de căutare

Noile generații de programe de e-mail oferă o facilitate utilă pentru căutări frecvente. După realizarea unei căutări, rezultatele pot fi salvate sub forma unor foldere virtuale, numite „foldere de căutare", acestea putând fi menținute „la zi", prin actualizări automate. Astfel, atunci când se doreşte reluarea căutării se va apela direct folderul de căutare, care conține deja e-mail-urile căutate.

Răspunsul automat (Autoresponder)

Acesta este de fapt o opțiune care furnizează instantaneu un răspuns automat, de fiecare dată când se primeşte un mesaj. Astfel, persoana care a trimis un e-mail la adresa respectivă va primi în câteva minute răspunsul automat pe care l-ați creat în autoresponder.

În acelaşi timp, dumneavoastră veți primi un e-mail de confirmare în care vor fi specificate:

- adresa solicitantului
- data şi ora la care a fost trimis mesajul
- alte informații introduse în mesajul persoanei respective

Înainte de instalarea unui autoresponder trebuie luate în considerare două aspecte:

1. Mesajul se va scrie folosind un editor text, ca de exemplu Windows Notepad sau Wordpad. Apoi, cu comenzile **Copy** şi **Paste** se va copia în formularul setat inițial.
2. În mesajul pre-format trebuie să nu existe mai mult de 60-70 de caractere pe linie, pentru a evita liniile prea lungi şi a putea fi citit mai uşor.

Mesaje de eroare e-mail

Atunci când mesajul electronic nu poate fi distribuit, expeditorul primeşte un mesaj automat în acest sens, mesaj care explică şi cauzele insuccesului. Exista trei motive obişnuite datorită cărora transmiterea poştei electronice eşuează:

- sistemul de poştă electronică nu poate găsi serverul destinatarului – „*Host unknown*" (acest lucru înseamnă că domeniul din adresa destinatarului este inexistent);
- destinatarul nu este cunoscut de acel server – „*Unknown user*" (domeniul este corect, dar pe serverul respectiv nu se afla un utilizator cu numele specificat în mesaj)[9];

> *From*: Mail Delivery Subsystem <MAILER-DAEMON@gov.ro>
> *To*: <ion.popescu@primarie.ro>
> *Date*: Sun, 9 Feb 2006 18:15:26 +0200
> *Subject*: Returned mail: User unknown

- Programul poate găsi atât serverul cât şi destinatarul, dar nu poate transmite mesajul. Iată câteva motive posibile:
    - rețeaua poate avea erori, făcând imposibil contactul cu sistemul aflat la distanță;

[9] În ultima vreme au apărut o serie de viruşi care simulează mesajele de eroare de acest fel, cerând utilizatorului să deschidă fişierul ataşat, pentru detalii. Nu deschideți ataşamentele acestor emailuri!

- sistemul aflat la distanță poate fi „mort” (poate avea, de exemplu, probleme hardware);
- sistemul aflat la distanță poate fi greşit configurat.

Cu toate acestea, faptul că nu primiți un mesaj de eroare nu înseamnă obligatoriu că e-mail-ul a ajuns la destinatar. Este posibil să existe întârzieri în transmiterea datelor sau datorită unor erori în redactarea adresei destinatarului mesajul să ajungă la altcineva. De aceea este bine ca pentru mesajele importante să folosiți opțiunea de confirmare de primire (care va indica faptul că mesajul a ajuns la serverul de e-mail al destinatarului) sau cea de confirmare de citire (prin care destinatarul confirma printr-un mesaj automat faptul că a citit e-mail-ul dumneavoastră)

1.3.2. Junk Mail şi evitarea sa

Junk Mail (poştă inutilă/nedorită) reprezintă atât mesajele spam (a se vedea mai jos), cât şi alte mesaje nedorite, indiferent de natura lor (de exemplu, mesaje prin care se încearcă răspândirea de viruşi informatici – a se vedea mai jos secțiunea „Securitate”, subsecțiunea „Viruşi”)

Spam şi junk mail

Termenul de Spam este utilizat la nivel mondial pentru a desemna o categorie aparte de Junk Mail – mesajele electronice nesolicitate (de obicei având caracter comercial)[10].

Principalele produse la care se face reclamă în aceste mesaje sunt: site-uri pornografice, programe de calculator, produse medicamentoase, conturi de cărți de credit – majoritatea acestor mesaje sunt în engleza şi pot fi menite sa înşele consumatorul

De asemenea, spam-ul mai promovează lucruri cum ar fi jocuri piramidale şi false propuneri de afaceri, cele mai celebre fiind „frauda nigeriană” („Stimate domn, am nevoie de bani de la dumneavoastră pentru a putea scoate 2 milioane de dolari care se află într-o bancă din Nigeria. În schimbul ajutorului acordat, veți primi 40% din aceşti bani”) şi „loteria” (mesaj prin care sunteți anunțat că ați câştigat la loterie o sumă mare şi vi se cer diverse date personale pentru a putea ridica acea sumă).

Stoparea Junk Mail

Un prim sfat pentru a ne feri de spam şi de efectele sale este să nu răspundem la aceste solicitări pentru a nu confirma astfel adresa de poştă electronică (multe astfel de mesaje sunt trimise la adrese neverificate în prealabil) şi să nu oferim date personale sau bani unor persoane necunoscute, oricât de tentante ar părea ofertele lor. Este de asemenea preferabil să nu deschidem ataşamentele mesajelor care par a fi „spam” sau care provin din surse nesigure.

Programele de e-mail mai recente oferă diverse facilități pentru detectarea şi filtrarea mesajelor de tip „junk mail”[11]. Aceste programe analizează e-mail-urile primite şi

---

[10] Din ce în ce mai multe state consideră acestă trimitere în sine o practicăSiguri ai grija de bebe neacceptată. În România, Legea comerțului electronic, nr. 365/2002, prevede în alin. 1 al art. 6 că efectuarea de comunicări comerciale prin poşta electronică este interzisă, cu excepția cazului în care destinatarul şi-a exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări.

identifică mesajele cu mare probabilitate de a fi junk mail, permițând apoi ştergerea lor sau mutarea într-un folder separat.

În plus, se pot nominaliza expeditorii care trimit în mod constant junk mail, pentru a bloca mesajele provenite de la ei. De asemenea, se poate alege afişarea doar a mesajelor provenite de la persoane cunoscute (acelea a căror adresa se regăseşte în agenda de adrese a programului).

În cazul în care programul de e-mail nu are această facilitate, se pot folosi terțe programe care să filtreze poşta electronică.

În ambele cazuri, este indicat să verificăm la câteva zile folderul în care au fost mutate mesajele „junk mail", pentru a recupera eventuale e-mail-uri care au fost greşit încadrate în această categorie.

1.3.3. Arhivarea e-mail-urilor

Este indicat să păstrăm e-mail-urile importante şi mai ales cele oficiale (la fel ca şi scrisorile oficiale) pentru eventuale activități conexe sau pentru cazul în care apar neînțelegeri ulterioare. Păstrarea acestora poate conduce la o acumulare de e-mail-uri care să îngreuneze munca sau chiar să încetinească programul de e-mail.

De aceea, este indicat ca e-mail-urile mai vechi, care nu sunt revizuite des, să fie arhivate separat de e-mail-urile curente. Majoritatea programelor de e-mail oferă funcții dedicate pentru arhivarea şi regăsirea mesajelor.

Fişierele ce conțin arhive pot fi copiate şi pe un dispozitiv de stocare adițional, pentru a avea o copie de siguranță. În funcție de numărul de e-mail-uri arhivate şi de dimensiunea fişierului, acest dispozitiv poate fi o dischetă, un CD etc. (a se vedea mai jos subcapitolul „Arhive şi copii de siguranță" pentru detalii despre arhivare şi dispozitivele de stocare cele mai recomandate).

1.3.4. Reguli de utilizare a corespondenței electronice

La fel cum există reguli de purtare a corespondenței în interiorul unei instituții, poate fi creat şi un regulament de utilizare a mesajelor electronice în corespondența de serviciu. Instituirea unei astfel de politici îndeplineşte două obiective:

1. Organizațional: angajații sunt instruiți cu privire la utilizarea adecvată a poştei electronice, ceea ce poate avea ca efect eficientizarea activității
2. Legal: conținutul mesajelor electronice intră sub incidența legii la fel ca orice altă corespondență

De aceea este util pentru instituții să introducă astfel de instrucțiuni care se pot referi, între altele, la:

- structura mesajelor electronice (astfel cum este detaliată mai jos)
- desemnarea persoanelor care să primească copii ale mesajelor transmise (cc: şi bcc:)

---

[11] Există şi programe care se pot instala pe serverul instituției, blocând astfel junk mail-ul înainte ca acesta să ajungă la utilizator.

- când şi cui i se redirecționează anumite mesaje
- utilizarea confirmărilor de livrare/citire şi soluționarea erorilor de livrare
- riscurile de securitate
- folosirea adresei de e-mail în scop personal.

Termenul de răspuns

Poşta electronică este folosită în general atunci când se doreşte un răspuns rapid. De aceea este indicat ca fiecare e-mail să primească un răspuns în termen de două zile lucrătoare. Dacă răspunsul presupune o documentare mai amănunțită, o soluție convenabilă este expedierea unui mesaj standard prin care încunoştințați expeditorul de primirea mesajului şi îi comunicați termenul în care va primi răspunsul detaliat.

Trebuie subliniat de asemenea că Legea nr.544/2001 privind liberul acces la informațiile de interes public prevede şi forma electronică drept modalitate de solicitare şi obținere a acestor informații, iar termenele de răspuns sunt aceleaşi ca şi pentru solicitările clasice, respectiv 10 zile sau cel mult 30 de zile de la înregistrarea solicitării, în funcție de dificultatea, complexitatea, volumul lucrărilor şi urgența solicitării.

1.3.5. Recomandări utile pentru corespondența prin e-mail

Este vorba de aspecte care nu sunt obligatorii, sau nu sunt soluții la probleme de utilizare a e-mail-ului în sine, dar prin folosirea lor se câştigă timp, iar scrierea mesajelor va fi mai simplă:

Destinatarul

- **Trimiteți mesajul potrivit la adresa potrivită**. Înainte de a trimite un mesaj, alegeți cu atenție adresa de destinație. Nu trimiteți la adrese colective (care includ mai mulți destinatari) mesaje destinate unuia singur dintre ei, ci scrieți-i pe adresa personală. Dacă, dimpotrivă, răspunsul îi vizează pe toți destinatarii mesajului inițial, atunci transmiteți mesajul către toate adresele vizate. Când scrieți unei instituții care are mai multe adrese de contact publice, asigurați-vă că, dintre adresele de e-mail ale instituției respective, adresa la care trimiteți un mesaj este cea mai indicată pentru problema pe care o ridicați în mesaj. În felul acesta nu-i veți deranja pe alții cu mesajul dumneavoastră şi mesajul va ajunge mai sigur la destinație. Folosiți câmpul cc: numai atunci când destinatarul trecut aici ştie motivul pentru care primeşte copia mesajului.
- **Evitați sa trimiteți mesaje nesolicitate**. – a se vedea mai sus secțiunea dedicată fenomenului spam
- **Evitați redirecționarea mesajelor nerelevante.** Nu trimiteți mai departe „scrisorile în lanț" („*chain-letters*"), chiar dacă avertizează asupra unor viruşi periculoşi sau fac apeluri umanitare ori promit îmbogățirea, mai ales dacă aceste mesaje conțin şi ataşamente. Majoritatea acestor mesaje intră în categoria de „*hoax*" (mesaje de dezinformare). Întrucât este foarte greu de aflat dacă informația este reală sau nu cel mai sigur este să ştergeți mesajul respectiv.

Subiectul

- **Găsiți un subiect adecvat** – dați mesajului o denumire care să fie semnificativă atât pentru dumneavoastră cât şi pentru destinatar
- **Gestionați adecvat importanța mesajelor.** Nu folosiți în exces opțiunea „high priority" sau atenționarea de „urgent" sau „important" în cadrul subiectului, pentru că riscați să pierdeți valoarea acestor opțiuni atunci când veți avea nevoie în mod real de ele.

Cuprinsul

- **Stabiliți de la început formatul mesajului:** culorile pentru fundal, mărimea şi culorile textului, sau - dacă nu vreți prezentări speciale ale mesajului, alegeți formatul text. În orice caz, formatele selectate trebuie să fie adecvate pentru textul scris. Alegeți un format adecvat care să poată fi vizualizat cu uşurință de toți utilizatorii (ex. html, rich text nu poate fi văzut de toți). **Evitați să aranjați textul în timp ce îl compuneți** – pentru economie de timp. Lăsați această operație pentru faza finală, după ce ați scris tot textul.
- **Plasați adecvat răspunsurile dumneavoastră printre pasajele citate.** Este bine să citați din mesajul primit pentru a-l ajuta pe destinatar să facă mai uşor legătura cu mesajul lui precedent. Cea mai indicată metodă este intercalarea răspunsului printre paragrafele din mesajul citat, astfel încât corespondentul va vedea imediat la care frază din mesajul său vă referiți:

> Stimate(ă) Domn/Doamnă,
>
> Referitor la cererea dvs. vă comunicăm următoarele:
>
> > Doresc sa aflu dacă autoturismul Oltcit cu numărul XXXXX a fost radiat din circulație sau nu
>
> Primăria Capitalei nu deține această informație.
>
> > şi unde mă pot adresa pentru a obține un certificat în acest sens.
>
> Vă rugăm să vă adresați la Brigada de Poliție Rutieră din str. Logofat Udrişte Năsturel, nr.9-15, sector 3.
>
> Cu stimă,
>
> Ion Popescu – Biroul de relații publice

- **Răspundeți tuturor întrebărilor adresate** – Dacă nu răspundeți tuturor întrebărilor din mesajul adresat, veți primi în continuare alte mesaje referitoare la chestiunile rămase nelămurite, ceea ce consumă atât timpul dumneavoastră cât şi cel al corespondentului, şi poate crea totodată nemulțumiri. Puteți preîntâmpina astfel de situații prin răspunsuri clare şi complete inclusiv la întrebări ce pot fi anticipate datorită legăturii strânse cu subiectul în cauză.

- **Evitați frazele lungi**. Folosiți paragrafe scurte şi spații între paragrafe, structurați ideile sau enumerările prin marcatori şi numerotări. Încercați să nu construiți fraze mai lungi de 15-20 de cuvinte şi mesaje mai lungi de 5-6 paragrafe. Corespondența prin e-mail este destinată unei comunicări rapide, ceea ce determină un stil de redactare diferit de cel al scrisorilor clasice.
- **Nu copiați dintr-un mesaj sau alt document fără permisiune.** Pe lângă faptul că este nepoliticos să faceți publică o comunicare adresată exclusiv dumneavoastră, poate exista riscul să încălcați prevederi ale legislației privind dreptul de autor în cazul în care nu cereți în prealabil permisiunea pentru reproducerea textului respectiv.
- **Nu transmiteți informații confidențiale**. Comunicarea prin e-mail este similară oricărei comunicări efectuate prin alte mijloace, astfel încât sunt aplicabile regulile referitoare la confidențialitate. De asemenea, este util să inserați la sfârşitul mesajelor o notă prin care să specificați natura şi răspunderea pentru conținutul mesajului.
- **Evitați sa scrieți tot textul numai cu majuscule**. Pe Internet, scrierea unui cuvânt numai cu litere mari este interpretată ca o scoatere în evidență a cuvântului, dar dacă scrieți un text întreg aşa, este ca şi cum ați striga. Este iritant pentru majoritatea utilizatorilor, deci scrieți normal textul, chiar dacă sunteți grăbit.

Semnătura

- **Pregătiți-vă o semnătura completă.** Puteți câştiga timp dacă vă definiți o semnătura pe care să o ataşați rapid la mesaj. Când adăugați semnătura la un mesaj, ea va fi introdusa acolo unde se găseşte cursorul. Dacă nu vreți ca destinatarul sa primească toate datele din semnătura, puteți şterge pe loc din ele, dar oricum folosirea semnăturii predefinite vă scuteşte de scrierea aceloraşi date la fiecare mesaj. Semnătura este echivalentul unui antet la o scrisoare. Ea trebuie sa fie scurtă şi să nu includă date confidențiale:

Model de semnătură:

========== *<=O bară de separare , față de textul mesajului;*

Ion Popescu
Director Executiv - Biroul Relații Publice
Primăria Municipiului Bucureşti
Bd. Regina Elisabeta nr. 47 sector 5
Tel. 305.55.00
e-mail: ion.popescu@pmb.ro

========== *<=O bară de încheiere a semnăturii .*

Ataşamentele

- **Ataşați de la început fişierele pe care vreți sa le trimiteți odată cu mesajul.** În felul acesta vă asigurați ca nu veți uita să le ataşați la sfârşitul compunerii mesajului.

- **Nu abuzați trimițând mesaje mari**. Chiar dacă destinatarul poate primi uşor mesaje mari, acestea pot provoca dificultăți (congestii de trafic) atunci când trec prin servere mai aglomerate sau cu performanțe mai slabe.
- **Comprimați fişierele într-un singur document arhivat.** Dacă trebuie să ataşați mai multe fişiere este util să le arhivați intr-un singur document, folosind utilitare de arhivare cum ar fi WinZip, WinRAR, etc.
- **Nu transmiteți ataşamente executabile.** În general ataşamentele cu extensia .exe conțin viruşi şi de aceea sunt şterse automat de server. Dacă este absolut necesar să trimiteți astfel de programe ca ataşament este bine să avertizați în prealabil destinatarul, pentru a fi sigur că mesajul este trimis într-adevăr de dumneavoastră şi este „curat"

Reguli în listele de discuții*

- Nu trimiteți mesaje publicitare pe listă sau care nu se încadrează în subiectul propus inițial
- Nu utilizați adresele de e-mail aflate ca urmare a subscrierii la aceasta listă în scopuri comerciale sau ca sa enervați o altă persoană
- Dacă deveniți membru al unei liste folosiți o săptămână sau două pentru a urmări discuțiile, tonul folosit şi abia apoi interveniți dacă credeți că aveți ceva de spus
- Evitați conversațiile agresive şi discuțiile în contradictoriu dacă scapă de sub control, întrucât acestea sunt dezagreabile şi pentru ceilalți participanți la discuții.
- Urmați indicațiile care de obicei sunt primite o data cu înscrierea pe listă
- Înainte de a trimite un mesaj gândiți-va că el va ajunge la TOȚI membrii. Verificați cu atenție adresa la care este trimis! De multe ori dacă se trimite un răspuns la un mesaj de pe o lista de discuții, acesta va merge la toată lista şi nu numai la persoana care l-a trimis.
- Nu citați din mesajul la care răspundeți decât ceea ce este necesar pentru identificare
- În momentul în care nu mai doriți să primiți mesaje de pe listă folosiți adresa prin care puteți părăsi grupul imediat şi pe care de obicei o găsiți fie pe pagina grupului, în mesajul de întâmpinare fie în partea de jos al oricărui mesaj primit de pe lista de discuții.

* pentru o prezentare mai detaliată a listelor de discuții v. cap. *2.2.7. Listele de discuții*

1.4. Administrarea spațiului pe disc

Calculatorul de serviciu împreună cu echipamentele periferice fac parte din rețeaua instituției în care lucrați şi sunt proprietatea acesteia. Pentru a le menține în stare de funcționare optimă este necesar să colaborați cu departamentul de tehnologia informației pentru instalarea şi utilizarea corectă a programelor şi echipamentelor de lucru. În cazul în care instituția nu are un astfel de departament, este bine să rețineți şi să efectuați singuri câteva operațiuni de rutină care vă pot ajuta să obțineți un randament mai mare pentru lucrul cu calculatorul.[12]

[12] Mai multe detalii, inclusiv informații despre alte operațiuni în lucrul cu calculatorul, se găsesc la http://www.muntealb.com

1.4.1. Spațiul pe disc

Pe măsură ce folosim calculatorul, hard-disk-ul se umple din ce în ce mai mult cu fişiere vechi, neactualizate, dintre care multe au devenit neimportante sau chiar inutile şi care ocupă spațiu .

Pentru a asigura o utilizare optimă a spațiului pe disc şi pentru a uşura organizarea şi regăsirea fişierelor, este recomandat să ştergeți fişierele care nu mai sunt de folos[13]. De asemenea, este recomandată arhivarea fişierelor vechi în locuri sigure, astfel încât acestea să poată fi regăsite cu uşurință ulterior.

1.4.2. Instalarea şi dezinstalarea programelor

În general programele sunt concepute în aşa manieră încât să fie uşor de instalat şi folosit. Cele mai multe procese sunt automatizate şi utilizatorul intervine doar pentru a indica funcționalitățile de instalat sau folderul unde se salvează fişierele programului.

Deşi procesele în sine nu sunt deloc complicate şi pot fi efectuate de orice utilizator, este bine să contactați în prealabil departamentul de IT pentru a evita probleme de compatibilitate cu programele celorlalte calculatoare din rețea şi cu alte programe specifice activității dumneavoastră.

1.4.3. Scanarea discului

Pe parcursul utilizării calculatorului, datele stocate pe hard-disk sunt inscripționate şi apoi şterse, ceea ce poate duce la un moment dat la erori de citirea datelor sau chiar la pierderea de informații.

Pentru a reduce riscul apariției unor astfel de erori este recomandabil să se folosească utilitarul de scanare a hard-disk-ului, care controlează fişierele pentru a depista erorile şi a le repara dacă e posibil.

1.4.4. Defragmentarea hard-disk-ului

Prin instalarea programelor şi ulterior folosirea lor, spațiului de pe hard-disk se umple cu date care sunt stocate în diverse porțiuni (partiții), reducând astfel viteza de lucru.

Pentru regruparea şi rearanjarea fişierelor în funcție de programele de care aparțin, astfel încât acestea să fie accesate direct şi mai rapid, există un program utilitar de defragmentare a hard-disk-ului.

Se recomandă efectuarea operațiunii de defragmentare în mod regulat, mai ales în cazul în care se instalează şi se dezinstalează des programe complexe care ocupă mult spațiu pe disc.

1.4.5. Arhive şi copii de siguranță

Pentru a preveni orice pierdere de informații, datele importante de pe hard-disk trebuie arhivate periodic (această operație se numeşte „back-up”) pe medii de stocare ce trebuie păstrate în condiții de siguranță (copii de siguranță).

Copiile de siguranță pot fi păstrate pe CD, DVD sau chiar pe Web,. La momentul necesar (în cazul extrem în care se pierd datele respective de pe computer) se pot

[13] Este în primul rând cazul fişierelor „temporare”, care sunt create de diverse programe în timpul lucrului şi care, după închiderea programului nu mai sunt necesare.

recupera aceste date de pe suportul ales. Alegerea suportului se va face deci în aşa fel încât să permită un acces rapid şi sigur la datele salvate (în cazul în care trebuie recuperate), cu un cost redus.

În general, cea mai folosită metodă în prezent este salvarea datelor pe suporturi de tip CD-RW sau DVD+RW (reinscriptibile), pentru că acestea au o capacitate de stocare relativ mare, viteză de scriere/citire ridicată şi respectiv un cost scăzut al discurilor. Pentru cantităţi mici de date capacitatea dischetelor (1,44 MB) este suficientă.

Depozitarea datelor se poate face şi pe Internet, fiind disponibile servicii specializate de stocare fie contra cost (de obicei pentru cantităţi mari de date), fie gratuit. Unele site-uri oferă şi servicii de management al documentelor (de ex. www.sanscarta.com). Pentru stocare temporară sau pentru cantităţi mici de date puteţi folosi servicii gratuite de tipYahoo Briefcase (http://briefcase.yahoo.com) sau cele de găzduire de site-uri (ex. www.home.ro).

Pentru siguranţă deplină, este bine să folosiţi mai multe medii de stocare diferite (atât CD-RW, cât şi Internet, dacă aveţi o conexiune adecvată). De asemenea, informaţiile trebuie actualizate în mod regulat.

Este foarte indicat ca la nivelul fiecărei instituţii să se creeze un regulament de utilizare a calculatorului, care să cuprindă atât aspecte legate de arhivare şi back-up, cât şi alte chestiuni, cum ar fi cele legate de utilizarea e-mail-ului sau cele privind confidenţialitatea şi securitatea (prezentate mai jos).

1.5. Securitate şi confidenţialitate

Internetul aduce o serie de avantaje pentru productivitatea muncii, însă în acelaşi timp pune o serie de probleme de ordin social şi juridic – cum ar fi, criminalitatea, securitatea, confidenţialitatea etc.

1.5.1. Securitatea

Ne-ar plăcea să credem că propriul calculator este ferit de pericole, atât din afara cat şi din interiorul organizaţiei. În realitate însă, există o serie de factori care pot periclita computerul nostru, ducând la pierderea sau furtul datelor şi, în unele cazuri, chiar la distrugerea calculatorului. Astfel, anumite persoane ar putea să spargă securitatea sistemului pentru a obţine informaţii sau a trimite viruşi, iar diversele programe „spion" (a se vedea mai jos) se instalează în sistem căutând date despre utilizator.

Având în vedere specificul activităţii fiecărei instituţii, de cele mai multe ori datele stocate în calculator au o valoare mult mai mare decât echipamentele ca atare şi de aceea securitatea şi integritatea acestora reprezintă o prioritate. Totodată, infectarea unui calculator conectat în reţea reprezintă un pericol şi pentru celelalte calculatoare şi deci pentru întreaga organizaţie.

De ce trebuie să ne protejăm? În ultimii ani, pe măsura generalizării Internetului, a crescut şi numărul de viruşi, aplicaţii malitioase etc. Este din ce în ce mai dificil pentru utilizator să se protejeze şi să scape de aceste probleme.

Principalele riscuri sunt:
viruşii şi troienii
programele spion
programele hijack-er
atacurile hacker-ilor
pierderea/furtul datelor

Putem să ne ferim de aceste riscuri, dacă urmăm câțiva paşi simpli pentru a securiza computerul, cum ar fi actualizarea permanentă a sistemului de operare, instalarea unui program antivirus şi a unui firewall, utilizarea de parole şi back-up-uri.

Atât riscurile cât şi principalele căi de apărare sunt descrise detaliat în cele ce urmează.

1.5.2. Riscuri

2 noiembrie 1988 a fost o zi importantă pentru securitatea Internetului. În acea zi un proaspăt absolvent al Universității Cornell din Statele Unite, Robert Morris Jr., a executat un program de tipul *vierme*, primul program care a afectat într-un mod foarte serios Internetul. În câteva secunde, mii de calculatoare de pe întreg teritoriul Statelor Unite au fost scoase din funcțiune de neobişnuitul program. Sute de rețele ale institutelor de cercetare, universităților, dar şi ale celor câteva companii care erau conectate în acea vreme la Internet au fost afectate.

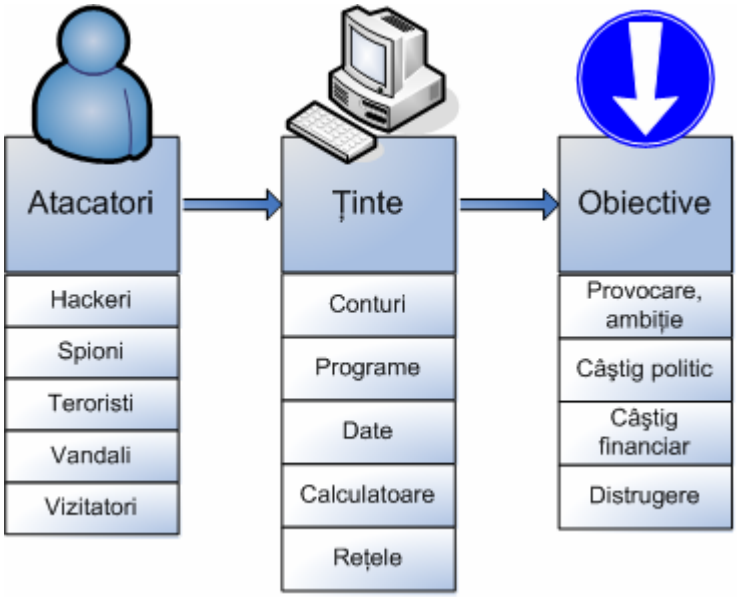
În decursul câtorva ore a fost format un grup de voluntari care să rezolve cât mai rapid această situație urgentă. Membrii grupului, denumit „Virus Net", comunicau cu ajutorul telefonului şi al segmentelor neafectate ale rețelei. În urma unui efort deosebit au reuşit să identifice cauza problemei, să izoleze programul virus şi să găsească o slăbiciune în codul acestuia. Această descoperire a făcut ca răspândirea virusului să fie oprită într-un timp record de 24 de ore de la apariție.

Deşi nu a avut efecte catastrofale, Internetul fiind format din foarte puține calculatoare la acea vreme (câteva zeci de mii, față de câteva sute de milioane câte sunt acum), acest incident a tras un serios semnal de alarmă în ceea ce priveşte securitatea sistemelor informatice în general şi a rețelelor în special.

Virusul lui Morris a revelat vulnerabilitatea Internetului şi a făcut să fie conştientizată nevoia de securizare a acestuia, având acelaşi efect asupra lumii informatice ca şi efectul primei deturnări a unui avion de pasageri, în 1960, asupra lumii aviației.

Pericolele informatice - introducere

În lumea reală există persoane care pătrund în case şi pot fura tot ce găsesc valoros. În lumea virtuală există indivizi care pătrund în sistemele informatice şi „fură" toate datele valoroase. La fel cum în lumea reală există oaspeți nepoftiți şi persoane care simt plăcere atunci când îşi însuşesc sau distrug proprietatea altcuiva, lumea calculatoarelor nu putea fi lipsită de acest fenomen nefericit.



El este însă mai greu de detectat şi de contracarat în lumea informaticii: dacă lipsa bijuteriilor se poate observa imediat, o penetrare a serverului de contabilitate poate fi depistată abia după câteva luni, când toți clienții au renunțat la serviciile firmei deoarece datele furate şi

ajunse la concurență au ajutat-o pe aceasta să le facă oferte mai bune.

Poveştile despre *cracker*i şi viruşi periculoşi constituie deliciul cărților şi articolelor de securitate informatică. Dar pericolul cel mai mare în ceea ce priveşte asigurarea acestei securități este de cele mai multe ori neglijat pentru ca că multe amenințări nu vin din exterior, ci din interior, factorul uman fiind în realitate veriga slabă.

Punctele vulnerabile exploatate

Vulnerabilitățile pot fi împărțite în şapte categorii principale:

1. Furtul de parole – metode de a obține parolele altor utilizatori[14];
2. Inginerie socială – convingerea persoanelor să divulge informații confidențiale;
3. Greşeli de programare şi portițe lăsate special în programe – obținerea de avantaje de la sistemele care nu respectă specificațiile sau înlocuire de software cu versiuni compromise;
4. Defecte ale autentificării – înfrângerea mecanismelor utilizate pentru autentificare;
5. Defecte ale protocoalelor – protocoalele sunt impropriu proiectate sau implementate;
6. Scurgere de informații – utilizarea de sisteme ca DNS pentru a obține informații care sunt necesare administratorilor şi bunei funcționări a rețelei, dar care pot fi folosite şi de atacatori;
7. Refuzul serviciului – încercarea de a opri utilizatorii de a utiliza sistemele lor.

Unelte

Unealta este o modalitate de a exploata vulnerabilitatea unui computer sau a unei rețele.

Principalele categorii de unelte folosite sunt următoarele[15]:

- *Atac fizic* (*physical attack*) – o modalitate de a sustrage sau distruge un calculator, o rețea, componentele acestora sau sistemele de susținere (ex: electricitate)
- *Viruşii* sunt mici fragmente de programe de calculator care se auto-replică sau inserează copii ale codului propriu în alte programe, atunci când este rulată o aplicație infectată. Un tip diferit de virus este „viermele” (*worm*) care nu infectează fişierele de pe disc, ci se răspândeşte cu ajutorul rețelei.
- *Troienii* sunt tot fragmente de programe însă nu au capacitatea de autoreplicare, fiind inserați în programe normale. Atunci când utilizatorul execută aceste programe, execută neintenționat şi fragmentul de cod de tip „cal troian”, aproape întotdeauna efectele fiind negative.
- *Script sau program* (*script or program*) – exploatare a vulnerabilităților prin execuția unui fişier de comenzi (script) sau a unui program.

---

[14] Este indicat să nu transmiteți parolele dvs. altor persoane şi să nu le păstrați scrise în zone unde mai au acces şi alții. Dacă parola dvs. a fost aflată de altcineva, este recomandat să o schimbați cât mai curând.

[15] Există o serie de alte modalități, mai puțin răspândite, de a ataca un sistem: schimbul de informații – obținerea de informații de la alți atacatori sau chiar de la oamenii care sunt atacați (prin inginerie socială); introducerea de comenzi într-un program; folosirea unui program sau a unui fragment de program cum ar fi viruşii şi viermii de rețea etc.

- *Programe spion* – sunt programe despre care utilizatorul nu are cunoştinţă, care se instalează odată cu alte soft-uri şi care rulează în paralel cu celelalte programe, culegând date despre utilizator.

Aceste unelte şi modul cum ne putem proteja de ele vor fi descrise în cele ce urmează:

A. Viruşii informatici

Datorită inteconectivtăţii şi caracterului său de reţea globală, Internetul a oferit mediul cel mai propice pentru răspândirea viruşilor informatici.

Denumirea de virus a fost consacrată datorită similitudinii cu viruşii biologici, având nevoie ca şi aceştia de un mediu propice pentru a declanşa acţiunea de infectare şi pentru a se răspândi şi multiplica.

Tipuri de viruşi

Deşi în mod curent se utilizează termenul de virus pentru a denumi o gamă mai largă de programe nocive, în sens restrâns virusul este un cod care se răspândeşte prin intermediul unei "gazde" (adică un fişier care poate fi transmis prin reţea sau pe un suport către alte calculatoare, infectându-le şi pe acestea la deschiderea fişierului.)

Virus	segment de program care se extinde prin ataşarea la un anumit fişier fără cunoştinţa utilizatorului. Poate infecta programe, documente şi componente ale sistemelor de operare.
Vierme **(Worm)**	program ce rulează independent şi se replică prin copierea automată de pe un calculator pe altul, de obicei în cadrul unei reţele sau prin ataşamente de e-mail.
Troian **(Trojan)**	program care rulează fără cunoştinţa utilizatorului; poate exploata breşele de securitate de pe staţiile victimelor. Cel mai des soseşte prin ataşamente sau de pe site-urile Web, de obicei deghizat în aplicaţii "hazlii" sau în diverse utilitare.

Ca regulă, viruşii nu afectează partea de hardware, ci numai programele şi datele stocate. Unii viruşi pot avea o acţiune întârziată, efectul nociv declanşându-se fie la un anumit moment în timp (*time bomb*), fie la executarea unei anumite comenzi în utilizarea normală a calculatorului (*logic bomb*)[16].

Deosebit de periculoase sunt programele de tip "troian". Acestea sunt programe de sine stătătoare şi în general nu se răspândesc. După cum sugerează şi denumirea, acestea se prezintă ca o aplicaţie utilă şi inofensivă, dar în realitate îndeplneşte alte funcţii, nocive, cum ar fi cedarea controlului asupra calculatorului, la distanţă, către o altă persoană decât utilizatorul legitim. Astfel de calculatoare "deturnate" se numesc "zombie".

[16] www.wikipedia.org

Răspândire şi metode de contracarare

La ora actuală, cea mai frecventă metodă de răspândire a aplicaţiilor malițioase este prin e-mail. Unele programe de e-mail protejează mesajele şi calculatorul prin blocarea automată a accesului la ataşamentele nesigure, precum şi prin filtrarea e-mail-urilor.

Deseori utilizatorul este păcălit să deschidă fişierul ataşat printr-un text din subiectul e-mail-ului sau printr-un titlu interesant al ataşamentului, cum ar fi o imagine sau un document.[17]

Datorită creşterii continue a numărului de programe nocive şi implicit a cazurilor de infectare, a devenit obligatorie instalarea de programe antivirus care să fie actualizate periodic pentru a beneficia de o protecție eficientă împotriva noilor viruşi. Aceste produse pot detecta şi elimina viruşii din fişierele descărcate şi avertizează utilizatorul în cazul descoperirii unui fişier infectat (vezi mai jos secțiunea 1.5.3. „Sfaturi pentru securizarea calculatorului").

B. Programele spion

Odată cu descoperirea potențialului comercial al Internetului, a apărut o nouă categorie de programe cu efect negativ asupra funcționării normale a sistemelor, chiar dacă nu sunt propriu-zis malware[18]. Aceste programe, denumite "spion", au rolul de a urmări obiceiurile utilizatorului atunci când navighează pe Internet şi transmit aceste informații către companii pentru ca apoi acestea să-şi direcționeze mai eficient ofertele comerciale către potențialii consumatori.

Programele spion nu se răspândesc la fel ca viruşii, ci se instalează pe calculator fără ştirea utilizatorului odată cu descărcarea de programe utile şi gratuite din Internet. Efectul cel mai vizibil este încetinirea vitezei de navigare pe Internet şi de rulare a unor aplicații curente. Unele programe pot redirecționa căutarea pe Internet, modificând rezultatele sau pot modifica setările din firewall, permițând instalarea unor programe indezirabile.[19]

De cele mai multe ori programul spion rămâne pe calculator şi funcționează chiar şi după ce se dezinstalează programul inițial cu care a fost asociat.

Pentru a verifica dacă aveți instalate astfel de programe spion[20] se pot folosi diverse programe utilitare[21]. Recent, firmele antivirus (Symantec[22], McAfee[23]) au adăugat produselor lor atribute anti-spyware.

---

[17] Ca o caracteristică aparte, e-mail-urile infectate cu viruşi mai recenți pot părea că provin de la persoane cunoscute (prin falsificarea identității expeditorului) şi pot chiar să conțină texte preluate din corespondența anterioară cu aceste persoane, inducându-ne să credem că ataşamentul este un document neinfectat.

[18] Denumire generică dată programelor nocive (viruşi, troieni, etc.)

[19] http://computer.howstuffworks.com

[20] Dintre programele de tip spyware, menționăm: Gator, KeyKey, SubSeven, Stealth Keyboard Logger, Snapshotspy, Surf Spy, Net Spy, GhostKeylogger, Pc Activity Monitor, PC Spy, STARR, Spector, Red Hand Pro, Hacker Whacker, FreeWhack, WinWhatWhere, BossEveryware, Conducent, Aureate.

[21] Unele gratuite, cum ar fi Ad-Aware sau SpyBot Search&Destroy

[22] www.symantec.com

[23] www.mcafee.com

C. Programele care "deturnează" browser-ul

Aceste programe sunt o varietate de spyware sau chiar viruşi, care realizează deturnarea („hijacking") unui program de la funcţionalitatea sa obişnuită, astfel încât acesta efectuează alte operaţiuni[24]. Atunci când afectează browser-ul, modifică pagina de start şi încetineşte viteza de navigare pe Internet.

Aceste programe se instalează la fel ca cele de spyware, fără ştirea utilizatorului, şi pot fi combătute folosind programe anti-spyware[25].

D. Atacuri ale "hacker"-ilor

Termenul de "hacker" se referă la persoanele care sunt acuzate de criminalitate informatică (cyber-crime). Aceste persoane folosesc diverse tehnici şi programe pentru a găsi breşele de securitate din calculatorul nostru fără cunoştinţa utilizatorului. Acest lucru se întâmplă cel mai adesea folosind un alt calculator din reţea şi folosind una din următoarele metodele: troieni, viruşi, viermi (a se vedea mai sus descrierea acestora), scanarea vulnerabilităţilor computerelor din reţea (în special cele în comunicarea cu alte computere), captarea parolelor (cu ajutorul unor programe numite "sniffer"), obţinerea directă a parolei cuiva (în cadrul unei conversaţii sau, pur şi simplu, prin urmărirea utilizatorului atunci când introduce parola respectivă).

E. Pierderea şi furtul datelor

Întrucât informaţiile existente pe un calculator sunt adesea deosebit de valoroase (în special datele secrete, confidenţiale), apare, la fel ca şi în cazul altor bunuri de valoare, riscul furtului acestor informaţii. Furtul se poate face prin accesarea fizică a calculatorului nostru, prin conectarea la bazele de date de pe serverul instituţiei, sau prin interceptarea unor convorbiri sau transmisii de date (deosebit de vulnerabile în acest sens fiind conexiunile prin unde radio – „wireless").

Un alt risc semnificativ constă în pierderea acestor informaţii de pe calculator. Aceasta se poate întâmpla ca urmare a unei ştergeri accidentale (sau rău intenţionate) ori în urma unor defecţiuni (în special ale sistemelor de stocare). Cea mai bună metodă de a pune datele importante la adăpost este crearea de copii de siguranţă, ceea ce permite recuperarea integrală a datelor chiar şi în situaţia în care o parte dintre ele au fost şterse sau modificate de acţiunea unui virus informatic. (a se vedea şi capitolul „Hard-disk management", subcapitolul „Arhive şi Copii de Siguranţă")

1.5.3. Sfaturi pentru securizarea calculatorului

Pentru a asigura securitatea calculatorului trebuie urmate câteva principii, cum ar fi folosirea de firewall-uri, programe anti-virus, filtre pentru e-mail şi parole. Principalele sfaturi pentru a asigura securitatea calculatorului sunt:

a. *Actualizaţi* mereu sistemul de operare
b. Instalaţi un *program antivirus* bun
c. Folosiţi un *Firewall*
d. Securizaţi *browser*-ul dumneavoastră

---

[24] www.wikipedia.org
[25] vezi www.spywareguide.com, www.spywareinfo.com

e. Descărcați programe numai din *surse sigure*
f. Nu deschideți *ataşamentele* suspecte ale e-mail-urilor
g. *Parolați* conturile, schimbați parolele şi nu folosiți aceeaşi parolă pentru toate conturile
h. Faceți *Backup* pentru datele importante

Trebuie menționat că în unele instituții există o persoană specializată în administrarea calculatoarelor şi a rețelelor (numit de obicei *administrator de sistem* sau *IT manager*). Printre atribuțiile acestuia se numără în cele mai multe cazuri şi asigurarea securității calculatoarelor, iar uneori şi aspectele legate de arhivare şi back-up. Dacă aveți o problemă legată de securitate, este indicat să apelați mai întâi la un astfel de specialist pentru a o soluționa.

Este recomandat ca în orice instituție să existe un astfel de administrator de sistem, sau o firmă externă, care să îndeplinească rolul acestuia atunci când e nevoie. În cazul în care nu puteți apela la un administrator de sistem, este indicat să urmați sfaturile detaliate mai jos, pentru a vă proteja calculatorul:

A. Actualizați mereu sistemul de operare

Actualizarea sistemului reprezintă alegerea şi instalarea celor mai recente componente, perfecționări, îmbunătățiri, actualizări de securitate şi drivere pentru computer. Aceasta actualizare trebuie să se realizeze cât mai des, astfel încât calculatorul să ruleze optim şi să fie cât mai puțin vulnerabil la atacuri sau viruşi.
Majoritatea programelor şi a sistemelor de operare pot fi actualizate vizitând pagina de web a acestora şi instalând cele mai noi componente, module etc. Sistemele de operare Microsoft Windows şi unele versiuni ale Linux (ex: Mandrake) oferă un program integrat în sistem, care atenționează automat utilizatorul despre apariția acestor componente noi şi facilitează instalarea lor (Actualizări Automate – Automatic Updates).

B. Instalați pe calculatorul dumneavoastră un bun program antivirus[26]

Programele antivirus[27] identifică viruşii cu ajutorul unei baze de date şi dacă, pe parcursul scanării, întâlneşte un fişier modificat de un virus atenționează utilizatorul, oferind posibilitatea de ştergere sau "corectare" a fişierelor afectate. Întrucât corectarea nu este întotdeauna posibilă (caz în care se pot pierde date importante), cel mai eficient mijloc de a vă feri calculatorul de acțiunea viruşilor este împiedicarea instalării acestora.

Pentru aceasta, țineți seama de următoarele recomandări:

- Scanați cu un program antivirus actualizat orice suport (dischetă, CD, DVD) pe care îl introduceți în calculator şi abia pe urmă folosiți datele stocate pe acestea

[26] Programele antivirus contribuie la protejarea computerelor împotriva viruşilor, viermilor, cailor troieni precum şi a altor "invadatori" care pot ataca un computer.
[27] O serie de programe antivirus sunt disponibile gratuit pe Internet, însă pentru computerele care utilizează frecvent Internetul şi poşta electronică recomandăm achiziționarea unor programe mai complexe, care oferă facilități suplimentare şi o protecție mai completă.

- Scanați toate fişierele descărcate de pe Internet şi cele primite ca ataşament prin e-mail înainte de a le deschide sau salva în calculator.
- Păstrați programul antivirus în funcțiune pe toată perioada sesiunii de lucru la calculator, pentru ca acesta să monitorizeze automat fişierele în uz
- Actualizați în mod regulat programului antivirus astfel încât acesta să cuprindă definițiile viruşilor nou apăruți şi mijloacele de combatere a acestora. În prezent majoritatea programelor antivirus se actualizează on-line în mod automat.

C. Folosiți un program Firewall

Programele firewall sunt folosite pentru a proteja calculatorul de pătrunderi neautorizate şi de viruşi. Firewall-ul filtrează toate informațiile care vin şi pleacă spre/dinspre calculator, în funcție de anumite criterii prestabilite (destinatar/expeditor, tipul informației etc.).

Firewall-ul poate împiedica persoanele străine (de exemplu hackerii, dar şi programele create de aceştia, cum ar fi viermii şi anumite tipuri de viruşi) să intre pe computerul dumneavoastră prin Internet.

Utilizarea unui firewall este importantă în special dacă sunteți conectat în permanență la Internet (de exemplu când aveți o conexiune prin cablu sau prin linii DSL sau ADSL).

Un firewall poate lua două forme, software sau hardware. Cele hardware sunt mai rar întâlnite şi sunt în general instalate şi întreținute de administratorul de rețea. Pentru a instala un firewall software, se pot folosi programe gratuite (disponibile pe Internet) sau achiziționate[28], unele fiind chiar incluse în sisteme de operare mai recente.

D. Controlați ceea ce rulează în broswer-ul dumneavoastră

Când browser-ul descarcă un program pe calculatorul dumneavoastră, va căuta informații despre programul respectiv şi despre firma care l-a creat. În cazul în care aceste informații sunt găsite, veți fi întrebat dacă doriți să instalați programul în cauză. Dacă informațiile despre program nu sunt disponibile, instalarea obiectului este riscanta şi browserul vă va avertiza în acest sens.

Securitatea navigării în Internet poate fi crescută prin stabilirea nivelului de securitate a browserului, acesta putând bloca anumite programe sau putând cere confirmări pentru a permite rularea lor.

E. Descărcați programe numai din surse sigure

Este bine să limitați descărcarea şi instalarea de programe de pe Internet la strictul necesar şi acest lucru sa se facă din site-uri sigure[29]. Evitați să descărcați fişiere din

---

[28] Principalele firewall-uri software sunt: ISS: BlackIce PC Protection; Network Associates: McAfee Personal Firewall; Symantec: Norton Personal Firewall; Tiny Software: Tiny Personal Firewall; Zone Labs: ZoneAlarm

[29] Este chiar indicat ca pe calculatorul de la serviciu să nu instalați alte programe decât cele necesare pentru munca dumneavoastră.

grupurile de discuții publice, deoarece accesul la acestea este nelimitat şi riscul este pe măsură!

De asemenea, evitați să deschideți sau să descărcați ataşamente suspecte primite prin e-mail, mai ales dacă provin din surse necunoscute. Obişnuiți-vă să verificați cu un program antivirus absolut tot ce intra în calculator – de la dischete şi CD-uri, pana la e-mail-uri şi ataşamentele acestora. Este întotdeauna mai indicat să previi decât să remediezi.

F. Nu deschideți ataşamentele suspecte ale e-mail-urilor

Aşa cum s-a arătat mai sus, cea mai frecventă metodă de răspândire a aplicațiilor malițioase este prin e-mail. Deseori utilizatorul este păcălit să deschidă fişierul ataşat printr-un text sau printr-un titlu interesant al ataşamentului, însă ataşamentul lansează în fapt un virus sau o altă aplicație malițioasă.

Ca atare, este indicat să nu deschideți ataşamentele despre care nu sunteți convinşi că sunt documente utile[30].

G. Parolați conturile, schimbați parolele şi nu folosiți aceeaşi parolă pentru toate conturile

Pentru a evita accesul unor persoane străine la calculatorul dumneavoastră, la diversele aplicații cu informații confidențiale sau la conturile de e-mail, este indicat să folosiți parole de acces pe care să le cunoaşteți numai dumneavoastră. Este indicat să folosiți parole diferite pentru diferitele conturi, astfel ca, în eventualitatea că o persoană străină descoperă parola pentru un anumit cont, aceasta să nu obțină automat acces la toate conturile dumneavoastră.

Câteva reguli de urmat la stabilirea de parole:

- nu folosiți:
  - numele dumneavoastră, al altcuiva din familie sau al animalului preferat,
  - elemente ale adresei dumneavoastră: numele clădirii, străzii, țării,
  - denumirea organizației, a proiectului etc.,
  - numărul de telefon, numărul de înmatriculare
  - numele starului sau personajului preferat (sau al filmului, cărții etc.),
  - cuvinte din dicționar;
  - numele contului pentru care stabiliți parola
- utilizați combinații de caractere mici şi majuscule, cifre şi alte caractere (de exemplu #, &, %, $, @);
- utilizați parole mai lungi de 6 caractere;
- schimbați parola de două ori pe an.

Care ar fi o parola bună şi care ar fi parolele de evitat?

- parola bună - %C26p03A1979$
- parole de evitat – aaa, hacker, primarie

[30] Trebuie evitate mai ales ataşamentele care conțin programe (acestea au în cele mai multe cazuri extensiile: exe, com, scr)

Pentru o siguranță sporită se pot folosi şi elemente hardware, cum ar fi cele de tip „token”[31], pe care le puteți purta asupra dumneavoastră şi fără de care calculatorul sau anumite programe nu vor putea fi pornite.

H. Faceți Back-up pentru datele importante

Întrucât există numeroşi factori de risc şi datele stocate pe calculator sunt adesea mai valoroase decât însuşi calculatorul, aceste date trebuie arhivate periodic – operație numită „back-up”. Această operațiune trebuie realizată frecvent (în funcție de importanța informațiilor, arhivarea se poate face lunar, săptămânal sau zilnic – în unele cazuri chiar mai des), deoarece datele pierdute sunt adesea imposibil de recuperat.

1.5.4. Confidențialitatea

Principalul avantaj pe care îl aduce Internetul constă în faptul că informațiile sunt disponibile tuturor. Însă acesta poate fi un inconvenient, atunci când este vorba de informațiile cu caracter personal, pe care nu dorim să le împărtăşim cu ceilalți (precum adresa de e-mail privată sau contul bancar). Problema poate deveni chiar mai gravă atunci când cineva foloseşte informațiile noastre personale pentru a face achiziții sau acte în numele nostru (furtul identității şi fraudă).

Din aceste motive trebuie să acordăm o importanță deosebită modului de prelucrare şi divulgare a datelor personale ale cetățenilor, respectiv modului în care aceştia sunt informați în legătură cu confidențialitatea datelor lor personale.

Confidențialitatea este abilitatea individului de a decide *când* şi *în ce condiții* pot fi dezvăluite datele sale personale (pentru alte detalii despre confidențialitate, v. *Anexa 3 – Securitate – Concepte de bază*).

Confidențialitatea în cadrul administrației publice

Confidențialitatea informațiilor personale este unanim recunoscută ca un drept fundamental al omului, protejat prin Constituția României — prevederile referitoare la ocrotirea vieții private şi la inviolabilitatea corespondenței. Indivizii trebuie să fie convinşi că informațiile despre ei (cum ar fi datele personale colectate de către instituțiile guvernamentale[32]) vor fi tratate corect. Odată cu trecerea la societatea informațională, o parte tot mai mare din date sunt colectate, stocate şi procesate electronic, iar apariția guvernării electronice şi a serviciilor livrate electronic au extins şi mai mult accesul instituțiilor publice la datele personale ale cetățeanului. Acest fapt creează, pe bună dreptate, o serie de temeri pentru cetățenii cărora li se cere să furnizeze aceste informații.

[31] Astfel de elemente de securitate (numite şi „chei”) se introduc de către utilizator în portul de imprimantă sau portul USB al calculatorului pentru a putea porni aplicațiile importante. Când pleacă de la calculator, utilizatorul păstrează asupra sa „cheia”, astfel că programele în cauză nu pot fi accesate în lipsa lui.

[32] Pentru a furniza servicii către public şi pentru a îndeplini diverse funcții, instituțiile publice colecționează şi folosesc numeroase informații despre cetățeni, cum ar fi: nivelul veniturilor şi al taxelor, proprietăți imobiliare, educație, cazier, permis de conducere, dosar medical etc.

Încrederea cetățenilor este crucială pentru succesul programelor de e-guvernare, iar securitatea şi confidențialitatea informațiilor sunt cruciale pentru a dobândi această încredere. Ca atare, guvernele care doresc să implementeze programe de e-government trebuie să protejeze confidențialitatea informațiilor pe care le colectează. Astfel, multe țări au adoptat o legislație specială pentru protecția datelor personale şi a confidențialității.[33] Această legislație se bazează pe câteva linii directoare, numite generic "practici corecte privind colectarea şi utilizarea informației":

- **Limitarea colectării**: Nu trebuie colectate mai multe informații decât cele strict necesare pentru efectuarea procesului sau tranzacției respective; toate aceste date colectate trebuie obținute prin mijloace legale şi corecte, cu atenționarea prealabilă a cetățeanului şi cu consimțământul său.
- **Calitatea datelor**: Datele personale colectate trebuie să fie relevante pentru scopul activității respective, să fie corecte, complete şi actualizate cât mai des.
- **Specificarea Scopului**: Când sunt colectate date personale, scopul acestora trebuie clar specificat, iar utilizarea lor ulterioară trebuie limitată la realizarea acelui scop.
- **Limitarea utilizării**: Datele personale nu trebuie dezvăluite, furnizate sau utilizate în alt fel pentru scopuri diferite de cele specificate inițial, decât eventual: (a) cu consimțământul cetățeanului sau (b) în spiritul legii.
- **Securitatea datelor**: Securitatea datelor personale trebuie protejată împotriva pierderilor sau accesului neautorizat, distrugerilor, modificărilor.
- **Transparența**: În general, nu trebuie să se colecteze date în secret. Ca politică generală, practicile şi procedurile legate de datele colectate trebuie să fie transparente – cetățeanului trebuie să i se dezvăluie existența, natura şi scopul bazelor de date, precum şi instituția responsabilă de administrarea lor.
- **Accesul cetățeanului**: Cetățeanul are dreptul să acceseze orice date pe care instituția le deține despre el. Acest acces include (a) confirmarea existenței/inexistenței datelor referitoare la cetățean; (b) obținerea de copii ale datelor privitoare la el într-un termen de timp, la un cost şi într-un mod rezonabil şi respectiv într-un format accesibil; (c) argumentarea eventualelor refuzuri ale accesării şi posibilitatea de a contesta aceste argumente; (d) posibilitatea de a contesta datele privitoare la el şi, în măsura în care contestația este justificată, posibilitatea de a şterge, completa sau corecta datele eronate.
- **Răspunderea**: Instituțiile care colectează date trebuie trase la răspundere atunci când încalcă principiile descrise mai sus

[33] În România Legea nr. 677/2001pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date şi Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice