GOMEZ
the finest premium brands

RISCURI CU PRIVIRE LA UTILIZAREA SERVICIILOR PRESTATE PE CALE ELECTRONICĂ

Persoanele care utilizează servicii prestate pe cale electronică pot fi expuse, în special, la următoarele riscuri:

Spam	Primirea informațiilor de publicitate nesolicitate (comerciale) pe cale electronică.
Malware	Software care este capabil după pornire, să infecteze fișiere într-un mod de auto-replicare, de obicei, fără a fi observat de către utilizator. Are diverse metode de acționare și efecte, ocupă spațiu RAM, CPU și spațiu pe hard disk.
Worm	Software cu capacitate de auto-replicare. Worm e-mail este un atac distructiv împotriva rețelei, care colectează toate adresele de e-mail găsite în programul local de e-mail și trimite sute de e-mailuri cu „vierme" într-un atașament invizibil.
Spyware	Software care spionează activitatea utilizatorilor pe Internet, care se instalează fără conştientizarea, consimţământul sau controlul utilizatorului.
Software rău intenționat	Software nedorit sau rău intenționat care efectuează acțiuni neintenționate de către utilizator, cum ar fi: troian, wabbit, rootkit, keylogger, backdoor, exploit.
Cracking/phishing („spargerea parolei")	Activitate care are ca scop compromiterea securității sistemelor informatice (cracking) și obținerea informaţiilor personale, de exemplu pentru furtul de identitate prin trimiterea unor mesaje electronice false asemănătoare cu cele autentice.
Sniffing	Interceptarea neautorizată, cu ajutorul sniffer-ului – este un program de calculator, folosit pentru a intercepta și a analiza datele, care circula în reţea.
Kryptoanaliza Criptanaliză	Căutarea deficienţelor sistemului criptografic pentru spargerea sau înlăturarea acestuia.
Utilizarea dispozitivelor ilegale	Implementarea unor dispozitive ilegale în sistemul teleinformatic și/ sau în rețeaua de telecomunicații de către alte persoane, care oferă acces neautorizat la servicii protejate.

Pentru a evita riscurile menţionate mai sus, Clientul trebuie să-şi echipeze dispozitivul de conectare la Internet cu program de antivirus actual și cu zid de protecţie (firewall). În plus Clientul trebuie să aprovizioneze poșta sa electronică cu un program care descoperă prezenţa virușilor în e-mail-uri și verifică datele importate înainte de a le deschide cu ajutorul modului de scanare a programului antivirus.