FOLOSIREA RAȚIONALĂ A EMAILULUI

Mare atenție: **Acest mesaj conține cîteva sfaturi utile referitoare la folosirea emailului. Este benefic pentru voi şi pentru toți ceilalți. Vă rog, găsiți-vă cîteva minute pentru a-l citi. Este important.**

1. Ce este un SPAM?

Este un mesaj publicitar sau ceva de genul "făceți-vă milionar în timp ce dormiți". Prin definiție, este un mesaj NESOLICITAT.

2. Cum "au aflat" adresa voastră?

Cel mai des, se "fură" adresele din mesajele care se trimit masiv, ca de exemplu, bancuri, informații politice, etc., şi care, la rîndul lor, sunt retrimise CU TOATĂ LISTA DE ADRESE DE EMAIL VIZIBILĂ. După care, culmea, listele respective se vînd sau se negociază cu alți spammeri (autori şi manipulatori de spam).

3. Ce-i de făcut pentru a evita spamul?

A. De fiecare dată cînd trimiteți un email la mai mult de **1 (un) destinatar**, şi nu este necesar ca aceştia să-şi vadă reciproc adresele, ca de ex. un banc, folosiți modul **BCC** (Blind Carbon Copy). Modul **BCC** face ca lista destinatarilor SĂ NU APARĂ în conținutul mesajului. **VĂ ROG DIN SUFLET, FOLOSIȚI ÎNTOTDEAUNA MODUL BCC!**

B. Atunci cînd dați un **FORWARD** (redirecționare) pe un mesaj, dedicați doar cîteva secunde pentru **A ŞTERGE TOATE ADRESELE** ce provin din emailul anterior.
CÎT SE POATE DE SIMPLU!

4. Ce sunt acele emailuri de genul "Salvați săraca fetiță bolnavă de cancer?"

Ei bine, toate, TOATE aceste emailuri care vă cer să faceți un **FORWARD** (redirecționare) sunt **O MINCIUNĂ**! Ştergeți-le! Atenție: unele dintre ele sunt virusate sau conțin alte "surprize" nedorite. **NICIO COMPANIE (ca MICROSOFT, de exemplu) nu donează bani pentru redirecționarea acestor mesaje. NICIODATĂ ŞI NIMENI nu o face!**

5. Şi viruşii?

Nu trimiteți şi nu deschideți (executați) fişiere **.exe** sau **.doc,** decît dacă sunteți siguri că provin dintr-o sursă de încredere. Acestea sunt modurile tipice de infectare cu virus. Nu este suficient să aveți un antivirus instalat, pentru că antiviruşii ÎNTOTDEAUNA sunt rămaşi în urmă. Iar într-o campanie de spam, viruşii se multiplică într-o zi cu milioanele, iar antiviruşii de-abia dacă încep să-i detecteze în cîteva zile, săptămîni sau chiar mai mult.

6. Şi ce se întîmplă cu linkul "REMOVE" dintr-un spam?

ESTE DE ASEMENEA O MINCIUNĂ! Adică, atunci cînd vi se trimite un spam (email nesolicitat) şi vi se spune că, dacă vreți să fiți eliminat de pe listă, să răspundeți cu REMOVE, este numai pentru a verifica, din listă, care emailuri sunt reale şi valabile. Răspunzîndu-le, în mod automat şi indirect nu faceți altceva decît să le confirmați că adresa voastră este reală, iar ei nu numai că vă trimit spam în continuare, ba chiar vînd adresa voastră de email altor spammeri. **NICIODATĂ să nu răspundeți, NICIODATĂ!**

7. Ce altceva pot să mai fac?

De fiecare dată cînd primiți un spam, puteți da un **FORWARD** (redirecționare) către adresa "**abuse**" a acelui domeniu. De exemplu, dacă primiți un spam de la **niceprice@shopping.com**, retrimiteți-l la **abuse@shopping.com** sau la **postmaster@shopping.com**. Acolo se vor ocupa ei de măsurile ce trebuie luate contra spammerilor.

NICIODATĂ să nu cumpărați nimic de la cei care vă trimit spam!

CEL MAI EFICIENT LOG-OFF...

8. Dacă eşti administrator de email, vizitează, te rog, webul următor, pentru a afla mai multe despre cum se combate spamul:

http://spam.abuse.net/

Dacă vei trimite acest mesaj şi altor persoane, nu uita să-l trimiți cu **BCC** (copie ocultă). De asemenea, **şterge adresa expeditorului**, căci dacă nu o faci, aceasta va rămâne înscrisă în corpul mesajului.

Stimați prieteni, altă gogoaşă a Internetului:

Povestea emailurilor în lanț.

Nu există nicio fetiță care moare de cancer, numită Amy Bruce, iar dacă ar exista, fundația "Make-a-Wish" NU va dona nimic, nimănui. Acest gen de emailuri este uşor de verificat, intrînd pe site-ul fundației şi căutînd detaliile. Dacă ar fi adevărat, fiți siguri că Amy s-ar afla pe site, cu o fotografie a ei, şi cu alte date. Intrați pe http://www.wish.org/home/frame_chainletters.htm, unde se tratează chiar acest "email în lanț" în particular.

Pentru a nu comite din nou aceste erori, şi pentru ca Internetul si căsuța noastră electronică să fie mai "curate".

Emailurile în lanț sunt instrumente folosite de către webmasterii paginilor porno, ale companiilor care vînd orice, ale cazinourilor online, ale agențiilor de "cîştiguri rapide", într-un cuvînt, firme care negociază şi vînd liste de adrese email, precum şi altele care se folosesc de spam pentru a exista.

Scopul "lanțurilor" este de a se (re)trimite ceva de genul:

1. Ajutor pentru un copil bolnav.
2. Cum că Ericsson/Nokia/Motorola fac cadou telefoane celulare.
3. "Virus nou: nu-l deschide!" (se numesc alarme false, sau hoaxes).
4. Bill Gates face cadou 5000$ şi o călătorie la Disney World dacă...
5. Despre tipul care s-a trezit dimineața în şanț, fără un rinichi.
6. Benzinării care explodează din cauza celularelor.
7. Ace de seringă infectate cu SIDA în cinematografe.
8. Sulfat de sodiu în şamponul tău.
9. Atacurile din parkingurile marilor centre comerciale.
10. "Vei avea mare noroc, cu cît trimiți mai repede şi la mai multe persoane acest mail".
11. "Retrimite-l la cît mai mulți, şi de asemeni celui/celei care ți l-a trimis ție, ca să-i arăți cît de mult îl/o iubeşti".

...şi multe altele care, în mod normal, apelează la sentimentele voastre umanitare, sau la dorința de a vi se împlini visurile, la speranța voastră că, trimițînd mai multe cópii veți avea mai mult noroc în viață, la frica voastră că anumite fapte (ca cele descrise în acele mesaje) vi s-ar putea întîmpla vouă sau celor apropiați, la dorința voastră de a trimite ştiri interesante sau glume prietenilor voştri, etc., etc., etc... pentru ca, mai apoi, chiar aceste emailuri să ajungă din nou la spammeri, "îmbogățite" cu sute şi sute de adrese de email, vizibile. Între ele, ale voastre şi a mea...
Iată de ce, la puțin timp, vom fi început să primim spamuri, al căror expeditor este, de exemplu, 9022ux5mz@wangabanga50245.com, sau oricare altul, oferindu-ne servicii sau produse de care nu avem nevoie.

Hackerii pot introduce prin email în calculatorul nostru celebrele programe Netbus sau BackOrifice, obținînd astfel controlul asupra PC-ului nostru, cu efecte profund maligne. Iar noi, fără să ştim, le retrimitem prietenilor nostri...
Există trei soluții de a opri aceste atacuri...

Cele trei soluții:

1. Nu dați **FORWARD** (redirecționare) pe **NICIUN FEL DE EMAIL ÎN LANȚ**. Este cea mai bună formă de a vă proteja prietenii.

2. Dacă totuşi vreți neapărat să dați **FORWARD**, cel puțin trimiteți emailul cu adresele destinatarilor scrise în modul **BCC** (Blind Carbon Copy, copie ocultă), şi **NU** în **TO** (către).
Scriind adresele destinatarilor în **BCC**, cei care primesc "lanțul" nu vor putea citi adresele celorlalte persoane cărora le-ați mai trimis emailul, iar astfel se frînează oarecum spamul.

3. Atunci cînd veți retrimite un email cu **FORWARD**, ştergeți mai întâi din noul email adresele posibililor expeditori anteriori. Altfel spus, nu lăsați scrisă în email nicio altă adresă, a nimănui, cu excepția propriei voastre adrese, exclusiv. Cel puțin, nu vom "dărui" spammerilor aşa de uşor adresele rudelor şi prietenilor noştri.
Acest mesaj este distribuit pe întreaga rețea de Internet, şi continuă să se distribuie, în beneficiul tuturor.

Răspîndeşte-l şi tu, dar cu adresele scrise în **BCC**!

Să luptăm pentru un Internet mai curat!