

Spamming in vraag gesteld

Geïllustreerde voorbeelden en praktische tips

November 2006



Spamming in vraag gesteld

**Geïllustreerde voorbeelden en
praktische tips**

November 2006

ON-LINE RAADPLEGING

Deze brochure kan gratis worden gedownload (in pdf-formaat) op de internetsite van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie :

Franse versie :

http://economie.fgov.be/information_society/spamming/home_fr.htm

Nederlandse versie :

http://economie.fgov.be/information_society/spamming/home_nl.htm

Duitse versie :

http://economie.fgov.be/information_society/spamming/home_de.htm

Engelse versie :

http://economie.fgov.be/information_society/spamming/home_en.htm

Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie

Vooruitgangstraat, 50

B - 1210 BRUSSEL

Ondernemingsnr. : 0314.595.348

<http://economie.fgov.be>

tel. (02) 277 51 11

Voor buitenlandse telefoons:

tel. + 32 2 277 51 11

Verantwoordelijke uitgever : Lambert VERJUS

Voorzitter van het Directiecomité

Vooruitgangstraat, 50

B-1210 BRUSSEL

België

Wettelijk depot : D/2006/2295/108

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

INHOUDSTAFEL

Voorwoord	5
Spam in vraag gesteld : geïllustreerde voorbeelden en praktische tips	7
DEEL 1 : SPAM MET HOGEGEVAARLIJKHEIDSGRAAD	11
1. De Nigeriaanse brief of « Afrikaanse scam »	11
2. « Phishing » of vissen	17
3. Elektronische berichten waardoor u gegarandeerd geld verliest	22
4. Elektronische berichten die gespecialiseerd zijn in valse en namaakproducten	26
5. Elektronische berichten die weinig inzitten met uw gezondheid	32
6. Elektronische berichten die informatica-virussen verspreiden	36
7. Elektronische berichten die de klassieke gevallen van oplichting behelzen	39
DEEL 2 : ONGEVRAAGDE ELEKTRONISCHE BERICHTEN MET BEPERKTE GEVAARLIJKHEIDSGRAAD	43
1. De « hoax », fopberichten of geruchten	43
2. Elektronische berichten die u – tegen uw wil – betrekken bij een publiciteitscampagne voor virale marketing	58



« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

VOORWOORD

Deze brochure stelt de meest voorkomende voorbeelden van spam voor die o.m. oplichting of (soms goed georganiseerde) informaticacriminaliteit inhouden.

Het gaat om die spam die ernstige hinder kan veroorzaken, die u veel geld kan doen verliezen of zelfs een gevaar kan uitmaken voor uw gezondheid, als u naïef genoeg bent om erop in te gaan.

Een deel van deze brochure is eveneens gewijd aan bepaalde technieken van verzending van ongevraagde e-mails die weliswaar minder gevaarlijk zijn dan de klassiekere spam, maar die, in bepaalde gevallen, moeilijkheden kunnen geven vanuit het standpunt van de toepassing van de wet.

De lijst van voorbeelden is niet volledig, maar poogt de meest voorkomende technieken voor te stellen, deze te illustreren en praktische raad te verstrekken, zodat u niet op uw beurt in de val trapt.

Deze brochure werd opgesteld door Didier GOBERT in het kader van de strijd tegen spam gevoerd door de FOD Economie, KMO, Middenstand en Energie, alsook in het kader van de samenwerking in de informele denktank SpamSquad (www.spamsquad.be). Ik wens hem te danken, alsook de collega's van de Algemene Directie Regulering en Organisatie van de Markt, van de Algemene Directie van Controle en Bemiddeling, van de Algemene Directie van Economisch Potentieel van de FOD Economie, de medewerkers van de Algemene Directie Geneesmiddelen van de FOD Volksgezondheid, en tevens de leden van de groep SpamSquad voor het aandachtig nalezen en hun constructieve opmerkingen.

Ik hoop dat u zich, dankzij deze brochure, niet (meer) zal laten beetnemen.

Een verwittigd mens is er twee waard !

Robert GEURTS

Directeur-generaal van de Algemene Directie Regulering en Organisatie van de Markt



« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

SPAM IN VRAAG GESTELD : GEÏLLUSTREERDE VOORBEELDEN EN PRAKTISCHE TIPS

INLEIDING

De term spam wordt vaker gebruikt dan gedefinieerd. Er bestaat overigens een grote verscheidenheid aan « spam », die onder de toepassing van verschillende wetgevingen kunnen vallen (wet op de elektronische handel, wet tot bescherming van de persoonlijke levenssfeer, wet inzake informaticacriminaliteit, strafwetboek, wetten inzake consumentenbescherming, wet inzake reclame voor geneesmiddelen, enz.).

In de ruime zin van het woord, verwijst deze term naar de verzending van ongevraagde elektronische berichten (e-mails). Hoewel dit niet systematisch het geval is, zijn de kenmerken van spam globaal gezien de volgende :

- de ongevraagde berichten worden massaal en soms herhaaldelijk verstuurd ;
- het bericht heeft soms een commercieel doel (de promotie van een product of van een dienst) ;
- de adressen worden vaak zonder medeweten van de eigenaar ervan bekomen (in strijd met de regels inzake de bescherming van de persoonlijke levenssfeer) ;
- bovendien gebeurt het vrij vaak dat, enerzijds, het bericht een onwettelijke inhoud heeft, bedrieglijk en/of schadelijk is en, anderzijds, de verzender zijn identiteit verbergt of een valse identiteit gebruikt.

De klassieke e-mail is weliswaar het meest gebruikt vehikel van de spammers, maar toch stelt men vast dat dit fenomeen zich meer verspreidt naar andere kanalen, zoals instant messaging (dan heeft men het over « spim »), blogs, sms, enz.

Deze brochure heeft een dubbel doel.

Ten eerste, strekt de brochure er eerst en vooral toe om voorbeelden van de meest voorkomende spam voor te stellen, die o.m. oplichting of (soms goed georganiseerde) informaticacriminaliteit inhouden.

Het gaat om die spam die ernstige hinder kan veroorzaken, die u veel geld kan doen verliezen en zelfs een gevaar kan uitmaken voor uw gezondheid, als u naïef genoeg bent om erop te antwoorden.

De lijst van voorbeelden is niet volledig. Immers, er blijken regelmatig nieuwe vormen van spam te ontstaan. Maar deze lijst poogt een voorstelling te geven van de verschillende gebruikte technieken, deze te illustreren en praktische tips te geven. Het doel hiervan is dat u niet op uw beurt in de val zou trappen.

Wij hebben ons beperkt tot de volgende gevallen :

1. De Nigeriaanse brief of « Afrikaanse scam » ;
2. « Phishing » of vissen ;
3. Elektronische berichten die u gegarandeerd... geld zullen doen verliezen ;
4. Elektronische berichten die gespecialiseerd zijn in... valse producten en namaakproducten ;
5. Elektronische berichten die weinig inzitten met uw gezondheid ;
6. Elektronische berichten die informatica-virussen verspreiden ;
7. Elektronische berichten die klassieke gevallen van oplichting behelzen.

8

Men kan zeker stellen dat deze soorten van spam een **hoge gevaarlijkheidsgraad** inhouden. Deze maken het voorwerp uit van het eerste deel van deze brochure.

De tweede doelstelling van deze brochure bestaat eruit twee praktijken van verzending van ongevraagde elektronische berichten te illustreren, waarvan de gevaarlijkheidsgraad veel lager ligt dan die van de klassieke soorten spam (hierboven bedoeld). Maar deze kunnen, in bepaalde gevallen, moeilijkheden stellen betreffende de toepassing van de wet of bepaalde risico's inhouden. Het gaat om de volgende twee praktijken :

1. De « hoax », fopberichten of geruchten ;
2. De elektronische berichten die u – tegen uw wil – betrekken bij een publiciteitscampagne van virale marketing.

Aan deze twee categorieën zou men een derde kunnen toevoegen : het gaat om de elektronische reclameberichten die worden verzonden door bedrijven die geacht worden ernstig te zijn, maar die desalniettemin de regels inzake voorafgaande toestemming, van identificatie van het publicitair karakter of van informatie betreffende het verzetsrecht niet hebben nageleefd.

Het gaat hier weliswaar om inbreuken op de wet en de overheid ziet erop toe om deze zoveel mogelijk te verminderen door, indien nodig, vervolgingen in te stellen. Maar men moet ook erkennen dat deze inbreuken, zoals ze worden voorgesteld in het eerste deel van deze brochure, eerder hinderlijk zijn dan een werkelijk gevaar vormen.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Deze derde categorie wordt niet behandeld in huidige brochure, want deze maakt reeds het voorwerp uit van de brochure « De spamming in 24 vragen & antwoorden » die on-line verkrijgbaar is op www.economie.fgov.be/information_society/spamming/home_nl.htm, waarnaar wij de lezer verwijzen.

Deze drie categorieën van praktijken stellen een **beperkte gevaarlijkheidsgraad** voor. Zij maken het voorwerp uit van het tweede deel van deze brochure.

Het is zeker niet onze bedoeling om een negatief beeld te geven van het internet of van e-mail. Het fenomeen moet overigens niet veralgemeend worden.

Het is evident dat e-mail alsmaar vaker dienst doet als het communicatiemiddel bij uitstek, omwille van zijn lage kost, snelheid en gebruiksgemak. Bovendien, vormt het internet alsmaar meer een nieuw platform waarop talrijke ernstige bedrijven handel drijven op dezelfde manier als in de werkelijke wereld, d.w.z. op volkomen correcte en eerlijke wijze.

Maar het is ook waar dat, zowel op het internet als elders, oplichters actief zijn en op zoek zijn naar slecht geïnformeerde of naïeve mensen om ze te « pluimen ». Wij hopen dat u, dankzij deze brochure, hiervan geen deel (meer) zal uitmaken...

Een verwittigd mens is er twee waard !

VOORAFGAAND : HERHALING VAN ENKELE VOORZICHTIGHEIDSBEGINSELEN !

Alvorens de concrete voorbeelden te behandelen, lijkt het ons aangewezen om enkele elementaire regels van voorzichtigheid in herinnering te brengen om de ontvangst van spam te vermijden of, minstens, te beperken :

- wees waakzaam wanneer u uw e-mailadres mededeelt en deel het niet zonder reden mee aan om het even wie ;
- vermijd uw e-mailadres te vermelden op een website, want dit zal systematisch worden gekopieerd door een programma van « automatic capture » van e-mailadressen dat wordt gebruikt door spammers ;
- indien u wil vermijden dat u « spam » krijgt op uw voornaamste e-mailadres (dat u gebruikt met uw naasten en in uw professionele relaties), maak dan een tweede adres aan bij een gratis provider. U kan dit adres dan gebruiken in het kader van toepassingen die riskanter zijn op het gebied van « spam » (inschrijving voor newsletters, deelneming aan forums, bestellingen op commerciële websites, vermelding op uw website, enz.) ;

- indien de oorsprong van het bericht of de identiteit van de afzender u duidelijk twijfelachtig lijken, vermijd dan te antwoorden op deze « spam », zelfs indien men u de mogelijkheid geeft om uw verzetsrecht uit te oefenen ! Vermijd ook te klikken op links die ingevoegd zijn in het bericht want spammers met kwade bedoelingen gebruiken deze technieken om na te gaan of uw e-mailadres nog actief is en... om u nog meer « spam » te versturen !
- maak de e-mailadressen van uw correspondenten niet zichtbaar wanneer u een groep of verspreidingslijst aanmaakt of wanneer u een e-mail doorzendt. U moet dus de adressen van alle bestemmingen verbergen in geval van gelijktijdige verzending van eenzelfde bericht aan verschillende personen. Gebruik daarom bij de verzending van een bericht de functie « blind copie » van uw e-mailprogramma, dat meestal wordt aangeduid door « Cci » of « BCC » of « CCC » ;
- deel de e-mailadressen van anderen (naasten, professionele kennissen, enz.) niet mede aan derden zonder de toestemming van eerstgenoemden ;
- als de afzender van het bericht niet duidelijk geïdentificeerd en gekend is, vermijd dan een bestand in bijlage van het bericht te openen (vooral als het de extensie .src, .exe, .scr draagt), want het kan gaan om een virus ;
- neem niet deel aan kettingmails ;
- installeer een goede firewall en een anti-virusprogramma, update deze regelmatig en scan regelmatig uw harde schijf(ven) ;
- maak uw kinderen vertrouwd met voornoemde regels en met het gebruik dat ze mogen maken van hun e-mailadres (best verschillend van het uwe !).

Voor zeer volledige informatiebronnen over spam en oplichterij via het internet, verwijzen wij de lezers naar enkele referentiewebsites:

- de website van de FOD Economie (www.economie.fgov.be), in het bijzonder de pagina m.b.t. de preventie van oplichterij (www.economie.fgov.be/protection_consumer/fraud_prevention/home_nl.htm), alsook de pagina met betrekking tot spam (www.economie.fgov.be/information_society/spamming/home_nl.htm) ;
- de website van de « Federal Computer Crime Unit » van de Federale Politie (www.fccu.be/crim/crim_fccu_nl.php) ;
- de website « SpamSquad » (www.spamsquad.be) ;
- de website « Consumentenbedrog » van het Onderzoeks- en Informatiecentrum van de Verbruikersorganisaties (www.consumentenbedrog.be) ;
- de website « Hoaxbuster » (www.hoaxbuster.com).

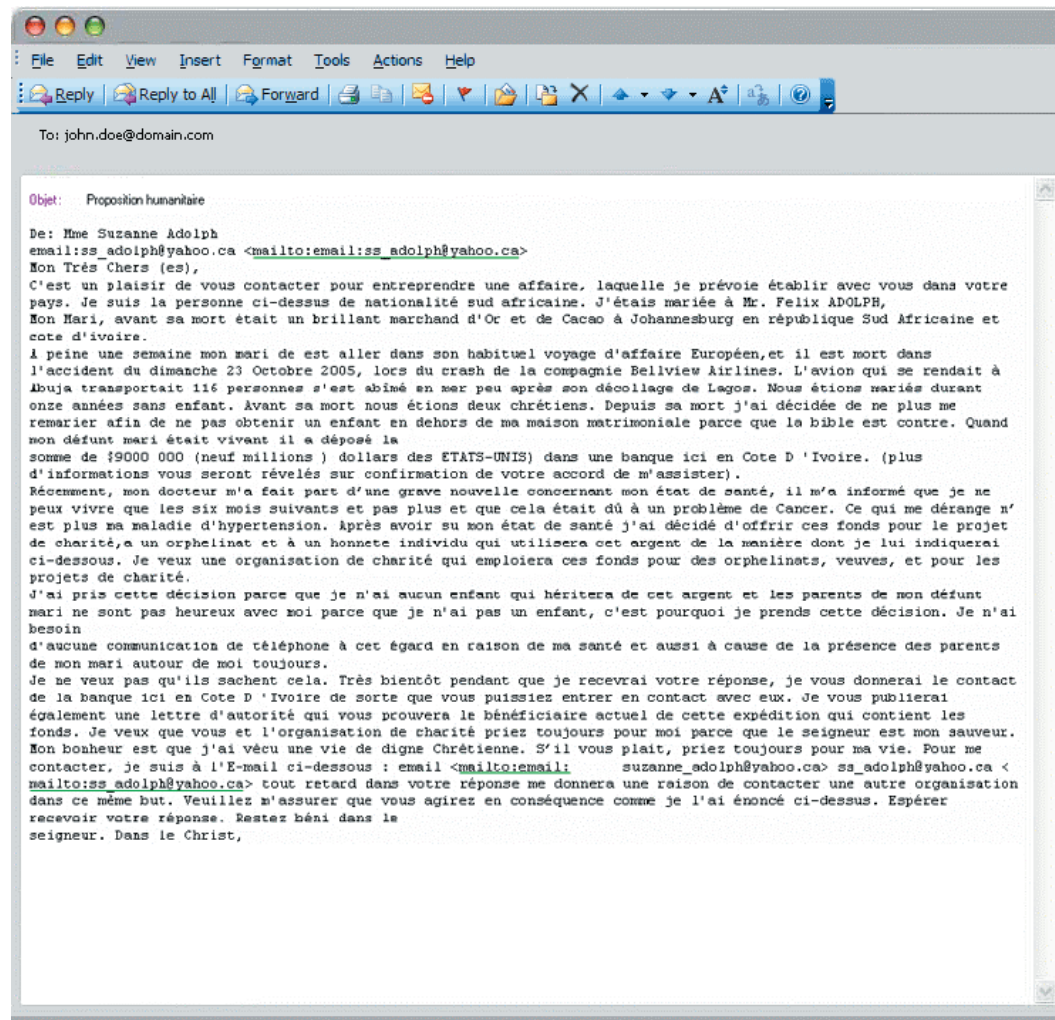
« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

DEEL 1 : SPAM MET HOGE GEVAARLIJKHEIDSGRAAD

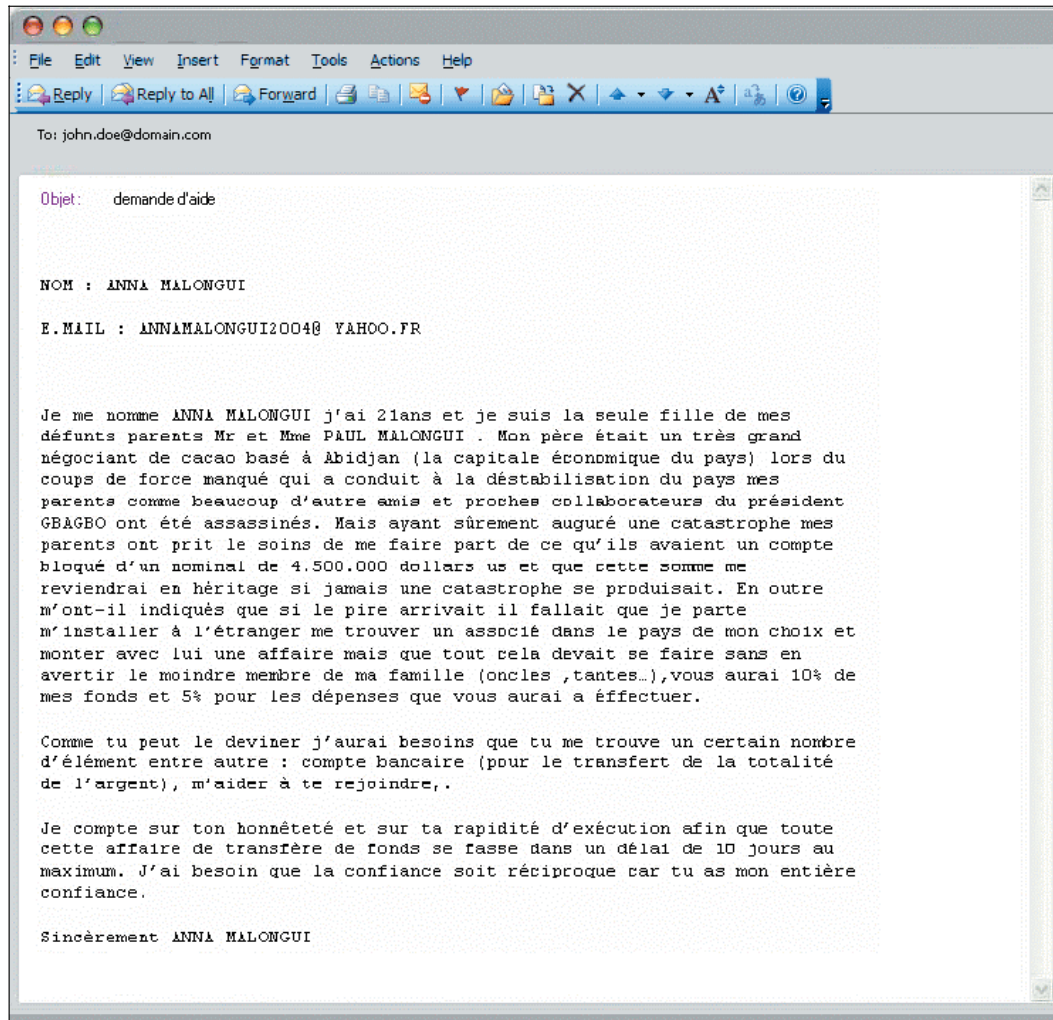
1. DE NIGERIAANSE BRIEF OF « AFRIKAANSE SCAM »

ILLUSTRATIES

Voorbeeld 1 van Nigeriaanse brief

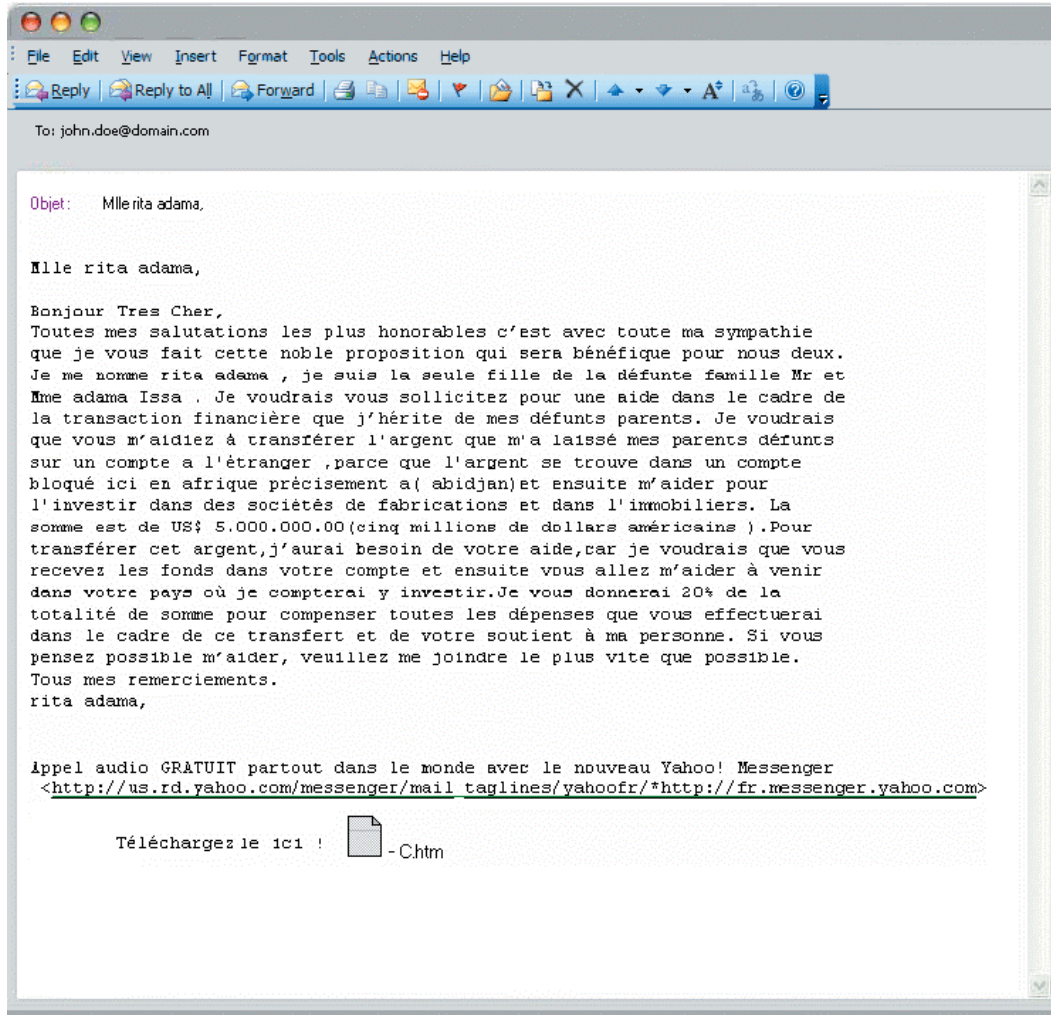


Voorbeeld 2 van Nigeriaanse brief

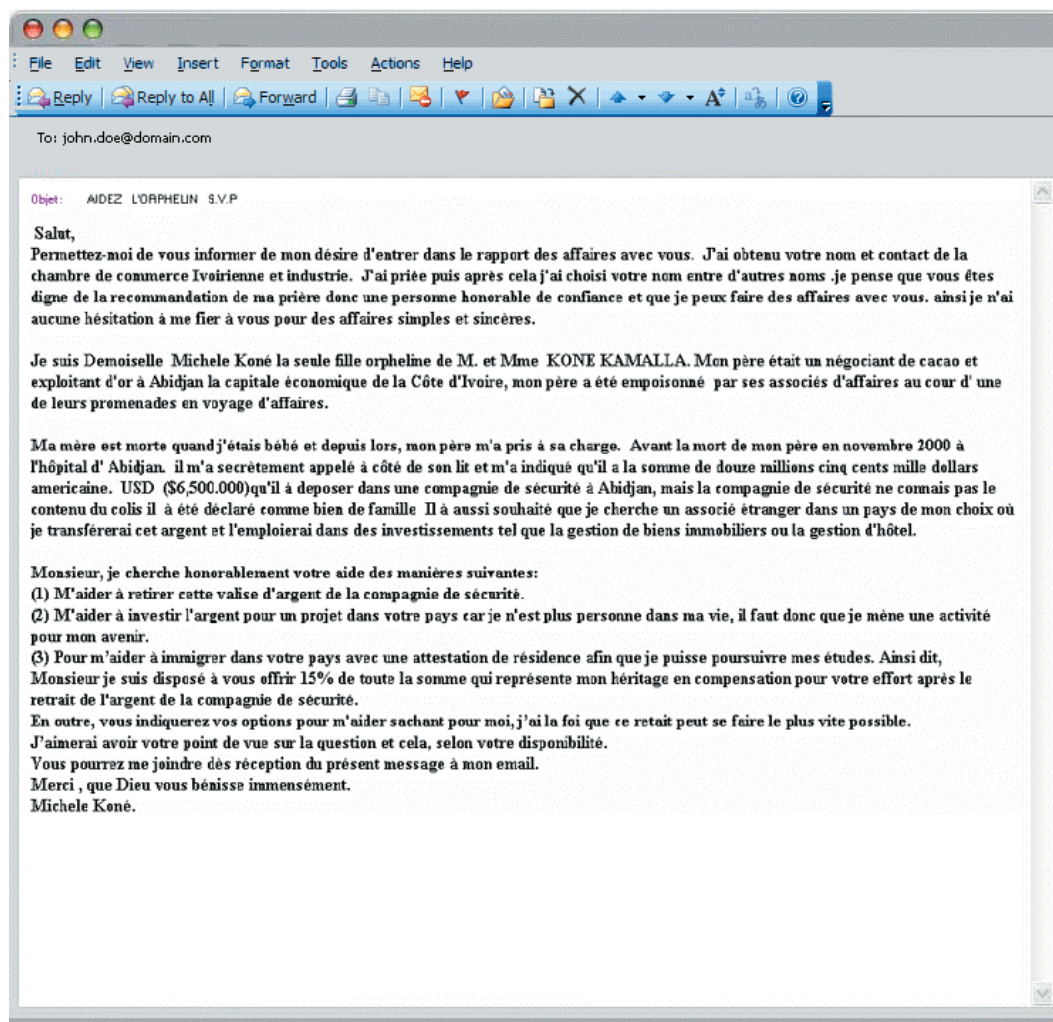


« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Voorbeeld 3 van Nigeriaanse brief



Voorbeeld 4 van Nigeriaanse brief



UITLEG

De Nigeriaanse brief of « Afrikaanse scam » is één van de oudste gevallen van oplichting via e-mail. Nochtans komt dit soort van bericht niet minder vaak voor. Het is uiteraard onmogelijk om alle gevallen op te nemen in deze brochure (er zouden op dit ogenblik zo'n 150 varianten bestaan !). Het leek ons echter nuttig om de voornaamste kenmerken ervan voor te stellen.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Of ze nu in het Engels, Frans of in andere talen zijn opgesteld, de berichten hebben vele punten gemeen:

- De auteurs stellen zich allemaal op identieke wijze voor (de ex-echtgenote van, de zoon van, de kolonel van, de broer van, enz. ... van een persoon die zogezegd bijzonder rijk is en net is overleden, verdwenen of in de gevangenis zit) ;
- De personen die u contacteren zijn allemaal in het bezit van een belangrijke som geld (of diamanten of goud enz.) die ergens is ondergebracht en die op u wacht om een geldtransfer te verrichten of de « schat » te deblokkeren ;
- Zij vragen uw hulp en beloven u om u in ruil rijkelijk te vergoeden voor de geleverde dienst.

Nochtans hebben zij allemaal hetzelfde doel : u geld afhandig te maken !

Indien u beslist te reageren op dit bericht, ontvangt u al snel alle details van de zaak en een verzoek om u wat meer te engageren. Opgepast echter : hoe meer u ingaat op het spel, des te moeilijker zal het worden om eruit te geraken en eens u erin zit, zet u veel op het spel.

De afzenders van het bericht zullen u bijvoorbeeld vragen om een rekening te openen bij een buitenlandse bank (een rekening die zal moeten gespijsd worden met een relatief belangrijke som), zelfs in uw eigen land (de rekening die op uw naam zal geopend worden kan dan gebruikt worden als transitrekening om geld wit te wassen !).

Het is ook mogelijk dat u geld zal moeten voorschieten om "bepaalde" advocatenkosten, rechten op transacties, taksen of smeergeld te betalen, om alle obstakels te overwinnen die tussen u en de enorme som geld die u werd beloofd zullen komen te staan.

De oplichters zouden uw rekeningnummer en uw bankgegevens ook kunnen gebruiken om valse overschrijvingen of valse cheques uit te schrijven op uw naam.

Uiteraard hoort u, nadat u deze bankrekening hebt geopend en/of deze geldsommen hebt betaald, niets meer van de afzenders en krijgt u uw geld en de beloofde som nooit (meer) te zien ! Het is bovendien mogelijk dat u wordt vervolgd voor medeplichtigheid aan een witwasoperatie.

HOE HANDELEN ?

Onze raad is eenvoudig, maar dwingend : antwoord vooral nooit op een dergelijke e-mail, die heel gemakkelijk te herkennen is en verwijder hem onmiddellijk.

Indien u, jammer genoeg, toch hebt gereageerd op een dergelijke mail, een eerste contact hebt genomen of zelfs nog verder bent gegaan, neem dan onmiddellijk contact op met de Federal Computer Crime Unit van de Federale Politie om de situatie uit te leggen op het adres : contact@fccu.be.

VOOR MEER INFORMATIE

De website : www.hoaxbuster.com ;

De website : <http://onguardonline.gov/spam.html> ;

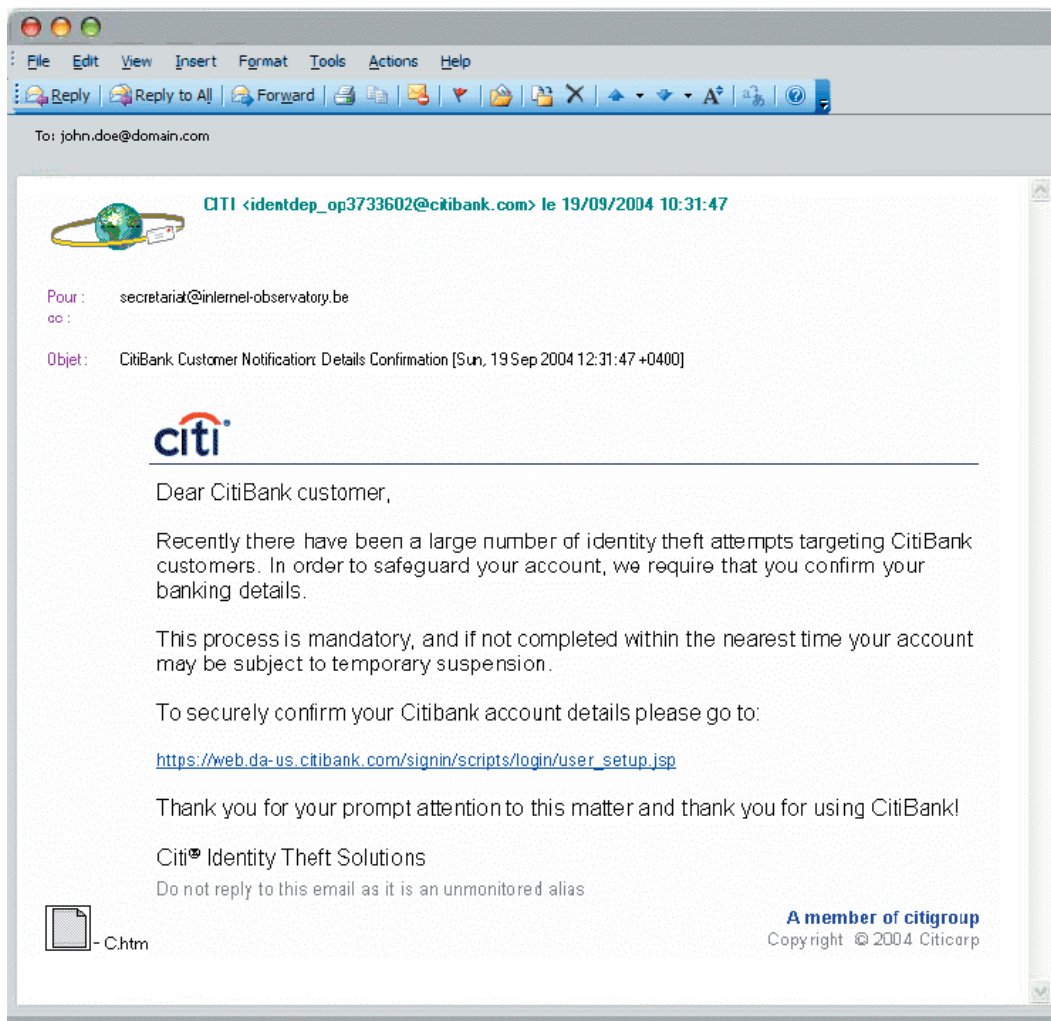
De website van de FCCU (Federale Politie) : www.fccu.be/crim/crim_fccu_nl.php.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

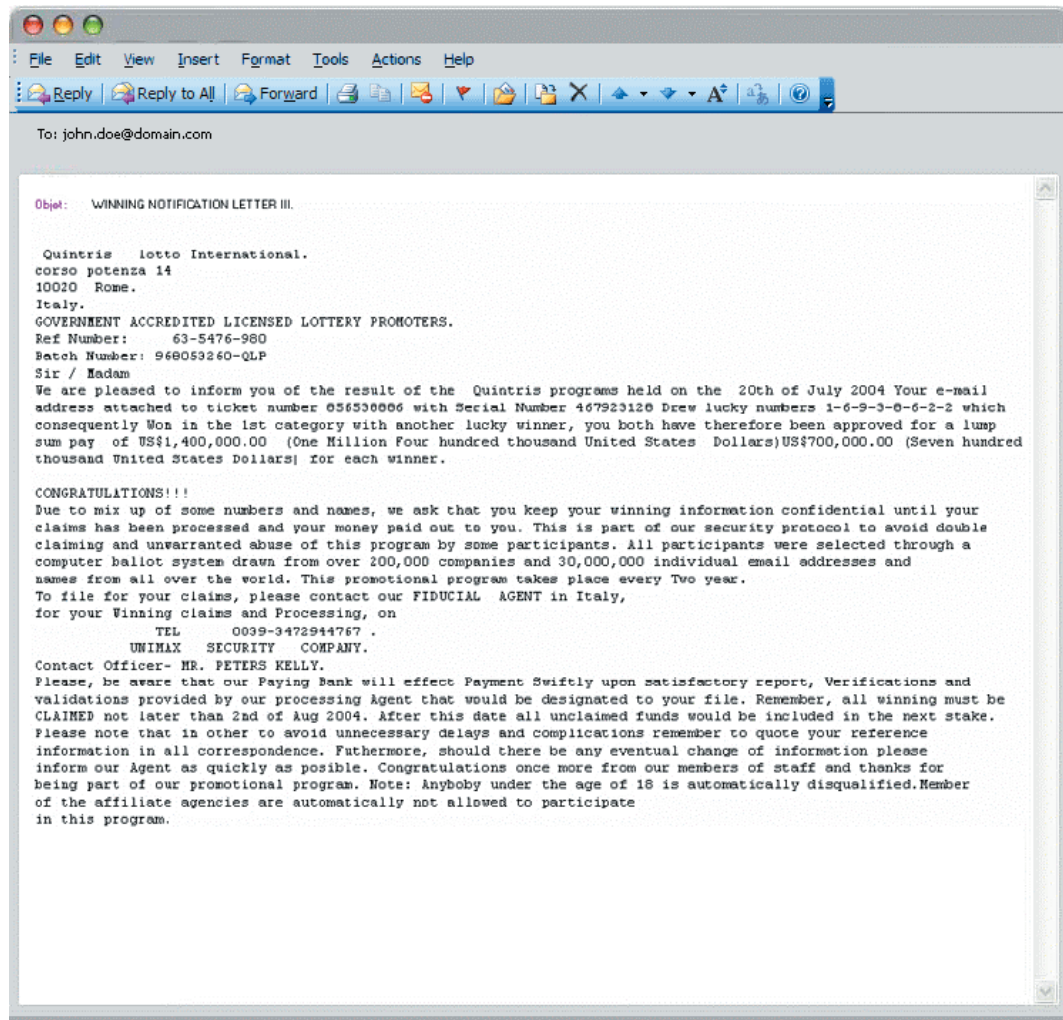
2. « PHISHING » OF VISSEN

ILLUSTRATIES

Voorbeeld 1 van « phishing »



Voorbeeld 2 van « phishing »



UITLEG

"Phishing", ook « vissen » genoemd, is een methode van oplichting die alsmaar vaker voorkomt via e-mail. Het woord « phishing » is in feite de samentrekking van het Engelse woord « fishing », in het Nederlands vissen, en « phreaking », waarmee men het hacken van telefoonnetwerken bedoelt.

Het gaat om een techniek die door hackers wordt gebruikt om persoonlijke informatie te bekomen van surfers (bijvoorbeeld de gebruikersnaam en het paswoord

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

en zelfs de bankgegevens) om ze frauduleus te gebruiken en dit, door de identiteit van een derde aan te nemen en een vals voorwendsel aan te wenden.

Of het nu gaat om het voorwendsel om persoonlijke gegevens te updaten op eBay, om na te gaan of de rekening van de consument bij Citibank of de internet provider niet werd gehacked, om zich ervan te vergewissen dat het kaartnummer van de Visa kredietkaart niet frauduleus werd gebruikt of andere dergelijke gekke scenario's, het doel van de oplichters is altijd hetzelfde : zich voordoen als een organisme of een betrouwbaar bedrijf dat beschikt over genoemde gegevens, de consument uitnodigen om on-line te gaan via een link en, om één of andere reden, laatstgenoemde ertoe brengen om zijn gegevens opnieuw in te schrijven in een formulier dat zich op een namaak webpagina bevindt, die een identieke kopie is van de originele site. Trouwens, de webadressen die in deze mails worden gebruikt, lijken soms heel erg op de officiële adressen.

In deze context, doen de uiterste hoogdringendheid, die meestal wordt ingeroepen, en het gemak waarmee de surfer snel naar de namaaksite kan worden gebracht, bepaalde mensen in de val trappen.

Eens de persoonlijke informatie in handen is van de oplichter, kan deze laatste er frauduleus van gebruik maken, o.m. om geld af te halen van de bankrekening van de bedotte surfer of om aankopen te doen met het nummer van diens kredietkaart.

HOE HANDELEN ?

Alleen al het feit dat u een e-mail ontvangt waarin u wordt verzocht om uw persoonlijke gegevens te updaten, moet uw argwaan opwekken.

Het is mogelijk dat dit soort van berichten wettelijk is, maar dat is bijna nooit het geval wat dergelijke gegevens betreft die zo gevoelig zijn als de gebruikersnaam en het paswoord of de bankgegevens, zoals het nummer van de kredietkaart. Ernstige banken vragen vertrouwelijke gegevens overigens ook nooit per e-mail aan hun klant.

Als de surfer een e-mail ontvangt, waarin hem om persoonlijke gegevens wordt verzocht, is de beste oplossing om niet te reageren en de mail te wissen. Als hij desalniettemin twijfelt, raden wij hem aan om rechtstreeks contact op te nemen met zijn dienstverlener (bankier, internet access provider, on-line verkoper, enz.) – waarvan de identiteit zou kunnen zijn gestolen – om de waarachtigheid van het verzoek na te gaan. In dat geval, moet men de eventuele contactgegevens die vermeld staan in de e-mail uiteraard niet gebruiken, maar betrouwbare gegevens bekomen via een andere weg.

Als de surfer er zich – te laat – rekenschap van geeft dat hij zijn bankgegevens heeft medegedeeld, moet hij eerst en vooral zijn rekening en zijn kaart zo spoedig mogelijk blokkeren zodat de oplichter er geen gebruik van kan maken. Het volstaat het nummer 070/344.344 te bellen (Card Stop). Deze dienst is beschikbaar voor alle Belgische bankkaarten, of het nu gaat om Bancontact/Mistercash kaarten of kredietkaarten. Wij raden ook aan om de feiten te melden aan de FCCU op volgend adres: contact@fccu.be.

Om te vermijden dat u in de val trapt, vindt u hieronder enkele controles die u kan verrichten om het twijfelachtig karakter van dit soort berichten te ontdekken :

- heb ik mijn e-mailadres medegedeeld aan dit bedrijf ? Indien niet, hoe komt het dat dit bedrijf mijn e-mailadres kent en mij via deze weg contacteert ?
- is het bericht in kwestie op naam ? Bevat het ontvangen bericht geïndividueerde elementen waardoor de waarachtigheid ervan kan worden geïdentificeerd (klantnummer, naam van het agentschap, enz.) ? Indien niet, opgelet !
- heeft de afzender een officieel e-mailadres ? Als het gaat om een yahoo- of hotmailadres, moet u deze e-mail als twijfelachtig beschouwen. Trouwens, men moet niet volledig vertrouwen op het e-mailadres van de afzender, vermits dit kan worden vervalst en soms een naam kan dragen die erg lijkt op dat van het gekende bedrijf ;
- men moet ook niet al te zeer vertrouwen op het voorkomen van de site waar naar men wordt geleid : een website kan tot de pixel toe worden gekopieerd !
- leidt de link in het bericht rechtstreeks naar het klassieke adres: [www.uw-bank.be], [www.uwdienstverstrekker.be], enz. ? Opgelet, vervalste sites hebben soms een adres dat erg lijkt op het officiële adres, maar niet volledig (controleer goed de schrijfwijze van de domeinnaam) !
- vermijd om rechtstreeks op de link in de e-mail te klikken, maar verbind u eerder met uw on-line dienst via de adresbalk van uw browser door zelf het adres te typen ;
- controleer of de site die de gevoelige gegevens bevat, beschermd is (dit is het geval wanneer het protocol https wordt gebruikt en er zich een hangslotje bevindt in de statusbalk onderaan de browser) ;
- laatste raad : verstrek nooit codes of identificatiemiddelen per e-mail.

Door het nemen van deze voorzorgsmaatregelen zou u heel wat nare verrassingen moeten kunnen vermijden. Maar eens u deze voorzorgen genomen hebt, moet u niet paranoia worden en in het achterhoofd houden dat het internet niet gevaarlijker is dan de werkelijke wereld waarin ieder van ons zich elke dag begeeft...

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

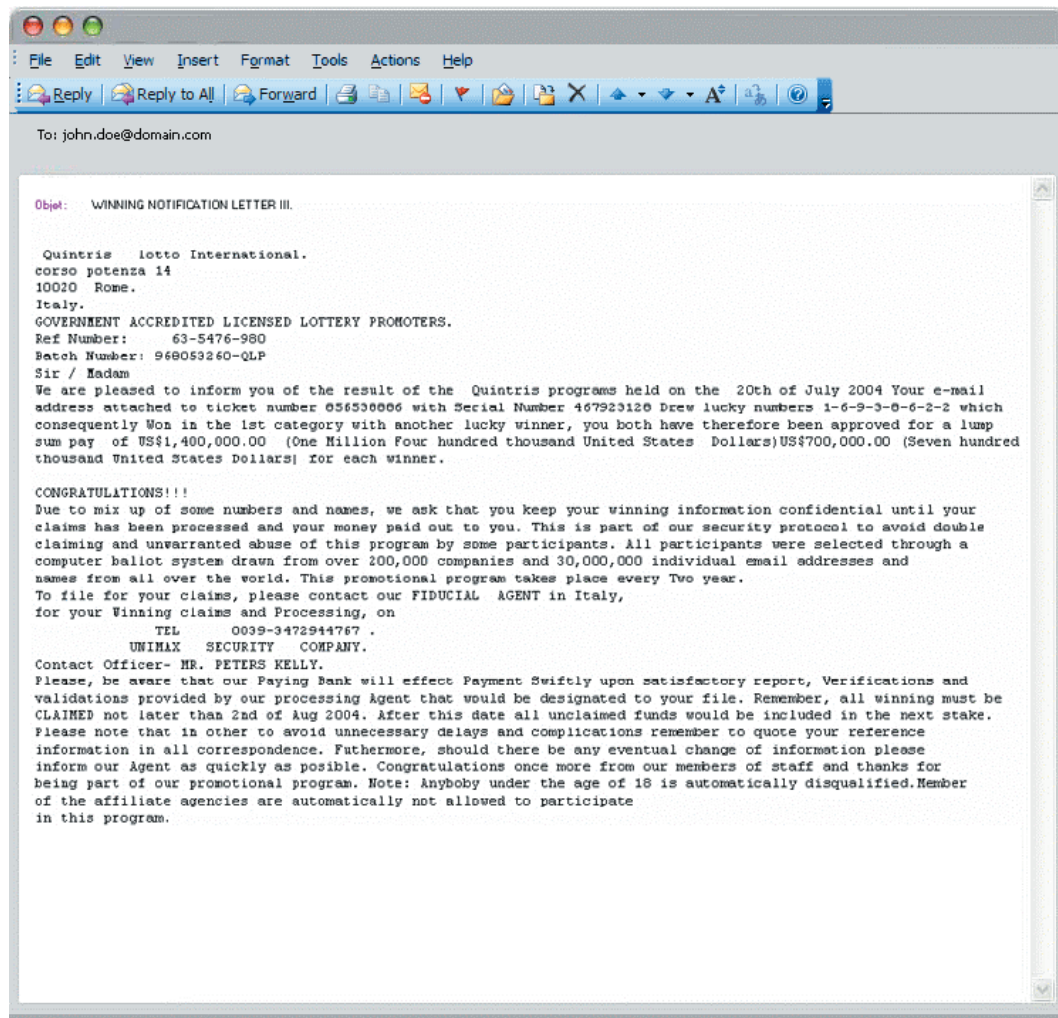
VOOR MEER INFORMATIE

De website « Consumentenbedrog » van het OIVO : www.consumentenbedrog.be ;

De websites : www.hoaxbuster.com ; <http://onguardonline.gov/phishing.html>.

3. ELEKTRONISCHE BERICHTEN WAARDOOR U GEGARANDEERD... GELD VERLIEST

ILLUSTRATIE



UITLEG

Internet heeft vaak de ontwikkeling of de wedergeboorte van oplichtingsmethodes, die ertoe strekken geld te ontfutselen aan de surfer, versneld. Er zijn talrijke varianten van deze oplichtingsmethodes. Wij beperken ons hier tot de bespreking van

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

degene die het vaakst voorkomen op het internet, te weten de valse loterijen, valse erfenissen en nep-verzoeken tot giften.

Voor de andere methodes, verwijzen wij de lezer naar de pagina gewijd aan oplichtingen van de FOD Economie

(www.economie.fgov.be/protection_consumer/fraud_prevention/home_nl.htm) en naar de uitstekende website : www.consumentenbedrog.be.

Valse loterijen

Niet zelden ontvangt men een bericht waarin wordt gemeld dat men, in het kader van een internationale loterij, een som geld gewonnen heeft, soms om en bij het miljoen euro. Om de winst te bekomen, meldt men u dat het volstaat uw rekeningnummer mede te delen aan de persoon die in de e-mail wordt genoemd. Het gebeurt zelfs dat een telefoonnummer wordt vermeld en dat een persoon aan het andere uiteinde van de lijn u de inhoud van de e-mail bevestigt !

In ieder geval, informeert men u dat u, om de winst te bekomen, de administratieve kosten en/of taksen moet betalen (het bedrag hiervan kan oplopen tot tientallen of zelfs honderden euro's).

In de grote meerderheid van de gevallen, gaat het om niet minder dan een poging tot oplichting :

- ofwel wordt het lot nooit bekomen, maar verdwijnt de oplichter in de natuur met de sommen die u hebt gestort ten titel van dossierkosten of taksen ;
- ofwel zal u een lot met een volkomen belachelijke waarde bekomen die in ieder geval minder is dan het bedrag dat u hebt gestort ten titel van kosten.

Soms hebben de oplichters zelfs het lef om de surfer een herinnering te sturen.

Inderdaad, enkele weken na de storting ter betaling van de administratiekosten, wordt de surfer telefonisch of per e-mail gecontacteerd door een beweerde verantwoordelijke van de gerechtelijke politie. Deze meldt de surfer dat het bedrag van de loterijprijzen in beslag werd genomen en dat de bestanden aantonen dat deze loterij de surfer een prijs verschuldigd is (overeenstemmend met de som die oorspronkelijk werd aangekondigd aan de surfer). Deze zogezegde verantwoordelijke van de politie biedt de surfer de mogelijkheid om de in beslag genomen prijs te bekomen middels storting van een kleine commissie...

Als de surfer zich een tweede keer laat beetnemen, achten de oplichters de kans groot dat hij dezelfde argumentatie nogmaals zal aanvaarden. Ze zullen dan een

tweede keer misbruik maken van de consument. Het is duidelijk dat hij de beloofde som nooit zal zien !

Een andere variante van deze oplichtingsmethode is de volgende : u ontvangt een veelbelovende e-mail. Men kondigt u goed nieuws aan: u wordt gevierd ! Uw e-mailadres werd uitgekozen om deel te nemen aan een wedstrijd! Om dit te doen, volstaat het een lot te kiezen tussen 25 en 400 euro en snel het nummer 0909 99 XXX te bellen.

In de hoop iets gewonnen te hebben – men weet immers maar nooit – belt u het telefoonnummer. Toevallig wint u niets, maar heeft de oproep u wel 25 euro gekost. Het gaat eenvoudigweg om een oplichting die gebeurt via een peperduur nummer.

De praktijken van deze bedrijven zijn eenvoudigweg illegaal. De wet van 14 juli 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument (WHP) verbiedt uitdrukkelijk alle reclame die bij de consument de hoop of de zekerheid wekt een product, een dienst of enig voordeel te hebben gewonnen of te kunnen winnen door de werking van het toeval.

Valse erfenissen

Hebt u nooit een e-mail ontvangen waarin u wordt geïnformeerd dat uw oom uit Amerika – waarvan u nog nooit hebt gehoord – pas is overleden. De persoon die u contacteert is zogezegd een openbaar ambtenaar die belast is met de nalatenschap, die u mededeelt dat u de enige erfgenaam bent van een kolossaal fortuin. Deze persoon deelt u echter mede dat, om over de erfenis te kunnen beschikken, bepaalde administratieve formaliteiten moeten worden verricht in het buitenland, waarvoor u voorafgaand dossierkosten moet betalen.

Zelfs op het internet, heeft Nonkel Amerika nog succes. De oplichters blazen aldus deze methode van oplichting nieuw leven in. Daar het bedrag van de gevraagde kosten bijzonder klein is (enkele honderden euro) ten opzichte van het kolossale fortuin waarover de erfgenaam zal beschikken, loopt hij met open ogen in de val en laat hij zich het bedrag van de dossierkosten afhandig maken.

Valse verzoeken tot giften

De Federal Computer Crime Unit – bijzondere afdeling van de Federale Politie – ontvangt regelmatig berichten betreffende potentiële risico's van wanpraktijken in verband met het internet.

Onder deze berichten, vindt men deels valse verzoeken tot giften, in het bijzonder tijdens de weken die volgen op grote evenementen zoals de Tsunami in Azië of de orkaan Katrina in de Verenigde Staten. Zo worden e-mails verzonden in naam van bekende niet-gouvernementele organisaties waarin de ontvanger wordt aangezet tot het doen van giften via het internet.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Het probleem is dat, in plaats van het geld over te maken op de rekeningen van de NGO, het wordt verstuurd naar een rekening in een exotisch land en de e-mails worden verzonden vanuit een al even exotisch land.

Achter deze solidariteitse-mails houden zich jammer genoeg oplichters verborgen die meer inzitten met hun eigen portefeuille dan met die van hun slachtoffers.

HOE HANDELEN ?

De surfer moet elk verdacht voorstel om gemakkelijk geld te verdienen en elke oproep tot gulheid aandachtig analyseren. Als voornoemde gevallen van oplichting zouden plaatsvinden in de straat en een onbekende hetzelfde voorstel zou doen aan de burger, dan zou deze onmiddellijk vermoeden dat er bedrog in het spel is. Waarom zou men dan onbekenden op het internet betrouwen ?

We herinneren er overigens aan dat het op het internet zeer eenvoudig is om de identiteit van een derde aan te nemen (bv. van bedrijven of organisaties die boven alle twijfel staan) of om e-mails te vervalsen : men kan dus maar beter systematisch zijn voorzorgen nemen.

In ieder geval, mag de surfer nooit enige administratiekosten betalen die men van hem vraagt om een zogezegd lot te bekomen dat men zou hebben gewonnen zonder deel te nemen aan het spel.

Als hij wordt gevraagd om een gift te doen, heeft hij er belang bij om zich tot de erkende nationale en internationale organisaties te richten en na te gaan of het opgegeven rekeningnummer overeenstemt met dat van de NGO in kwestie. Dit rekeningnummer kan gemakkelijk worden bekomen via andere media of via de (officiële) website van de NGO.

Indien u jammer genoeg in de val bent getrapt, raden wij u aan om de feiten aan te geven bij de FCCU op het volgende adres : contact@fccu.be.

VOOR MEER INFORMATIE

De website van de FOD Economie : http://economie.fgov.be/protection_consumer/fraud_prevention/home_nl.htm ;

De website « Consumentenbedrog » van het OIVO : www.consumentenbedrog.be ;

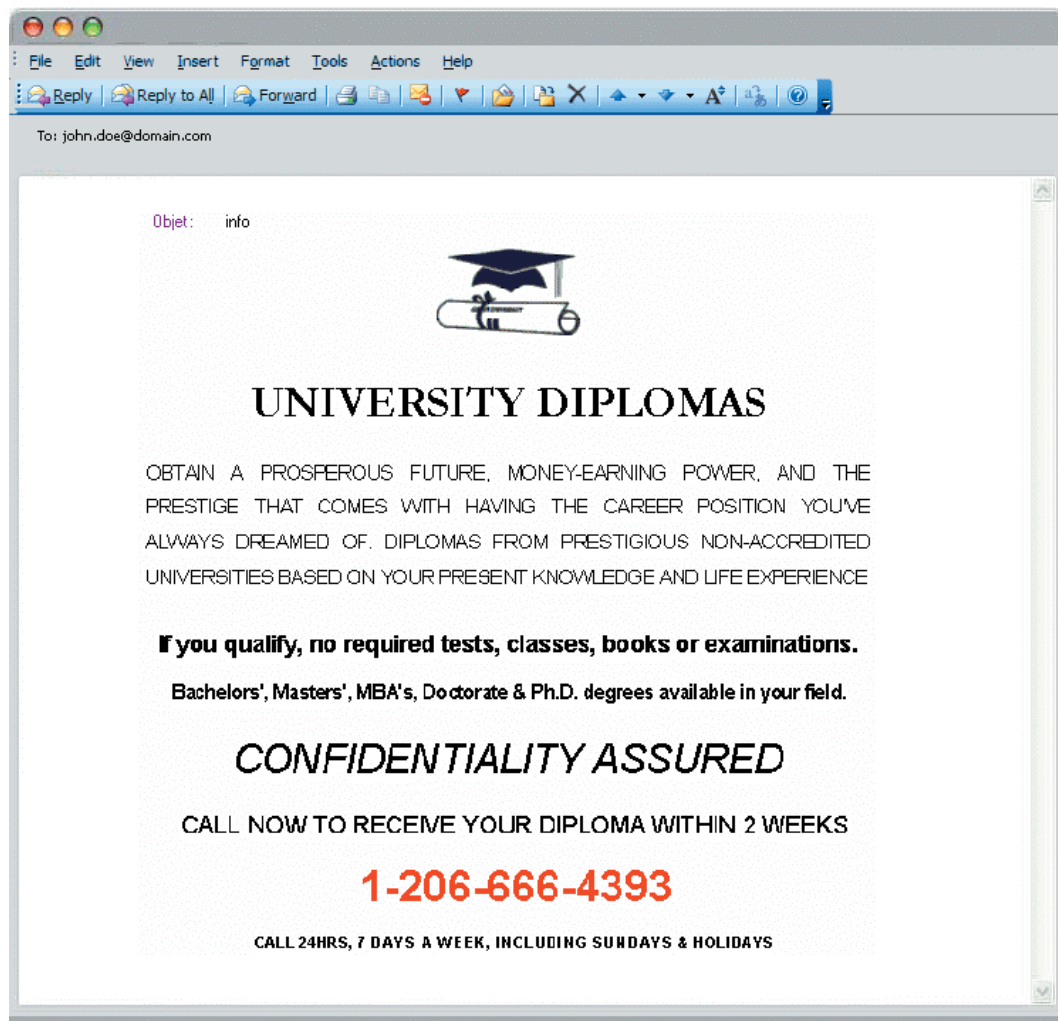
De website : www.hoaxbuster.com ;

De website : <http://onguardonline.gov/spam.html>.

4. ELEKTRONISCHE BERICHTEN DIE GESPECIALISEERD ZIJN IN... VALSE EN NAMAAKPRODUCTEN

ILLUSTRATIES

Voorbeeld 1: valse diploma's



« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Voorbeeld 2 : namaakhorloges



The image shows a screenshot of an email client window. The email header includes the recipient 'To: john.doe@domain.com' and the subject 'Objet: re [3]'. The main body of the email is a promotional advertisement for counterfeit luxury watches. It features a list of brand names on the left, a list of benefits on the right, a featured product 'Rolex Oyster Perpetual Submariner' with a price of '\$245.99', and a call to action at the bottom.

BUY YOUR ROLEX FOR ONLY \$245.99 !!!

Rolex
Tag Heuer
Vacheron Constantin
Patek Philippe
Omega
Officine Panerai
Jaeger-LeCoultre
IWC
Frank Muller
Chronoswiss
Cartier
Bulgari
Breitling
Audemar Piguet
A.Lange & Sohne

**BEST PRICES ON THE MARKET
JUST FOR YOU!**


A LOT OF MODELS!

GREAT DISCOUNTS!

LIVE SUPPORT!

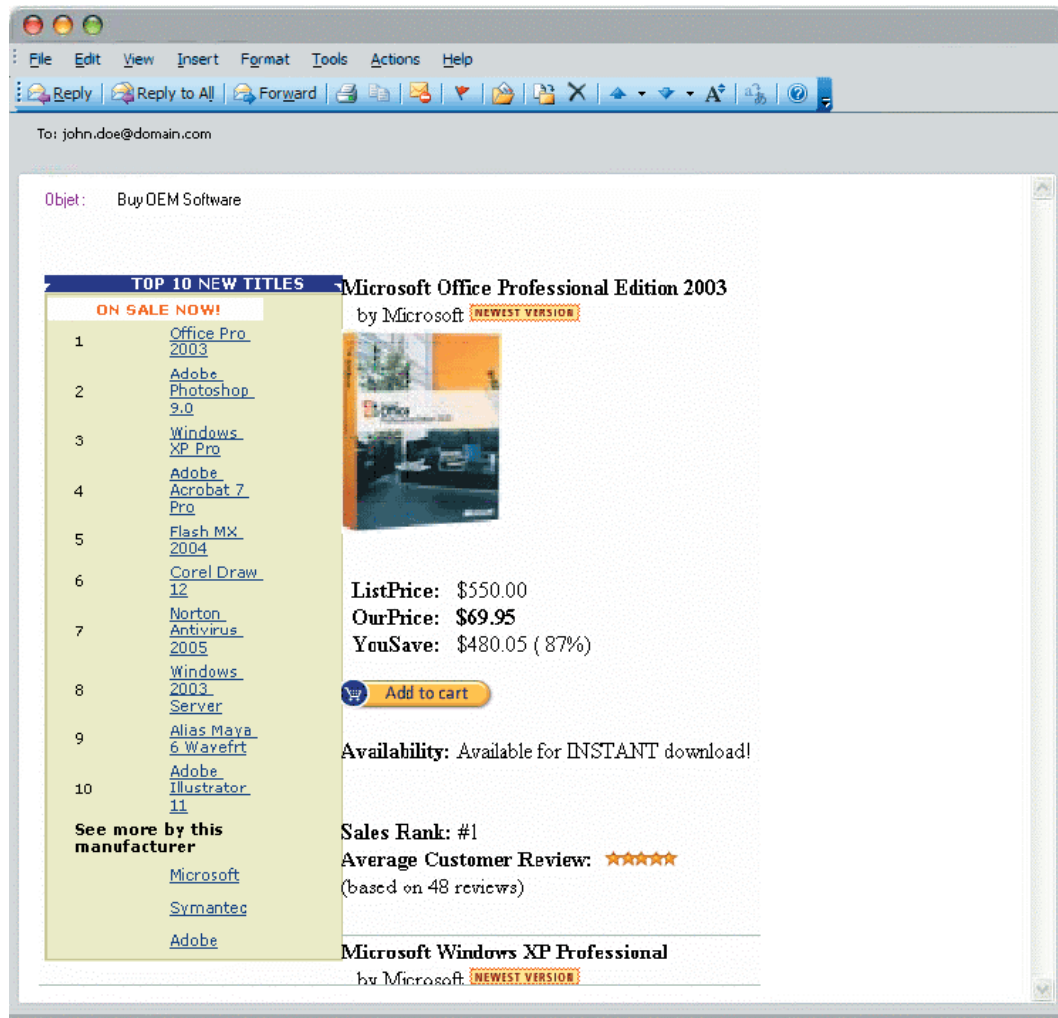
EXTENDED WARRANTY!

JUST ONE OF THE BESTSELLERS:
Oyster Perpetual Submariner

ROLEX  **\$245.99**

[CLICK ON THIS LINK TO VISIT OUR SHOP](#)

Voorbeeld 3 : namaakprogramma's



UITLEG

Op de markt vindt men vele namaakproducten en dit, in alle sectoren van de economische activiteit : cosmetica, juwelen, informatica, video, parfum, alcohol, textiel, marokijnwerk en zelfs de farmaceutische sector.

Met de term namaak bedoelt men, in de meest algemene zin van het woord, elke aantasting van een intellectueel eigendomsrecht.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Daar namaak een internationaal fenomeen is geworden, hebben de namakers al snel het belang van het internet in dit opzicht ingezien om namaak- of valse producten te koop aan te bieden.

Wie heeft nog nooit een e-mail ontvangen waarin men de aankoop voorstelt van een horloge, een programma, een diploma of van hi-fi materiaal en dit, tegen een prijs die niet te kloppen is door de concurrentie ? Het gebeurt zelfs dat de afzender in zijn bericht aanduidt dat het product eenvoudigweg vals is !

Specialisten van de strijd tegen fraude op het internet schatten dat spamberichten waarin namaakproducten worden voorgesteld vandaag de dag een belangrijk deel van de spam op wereldvlak voorstellen. Zelfs als slechts 0,001% van de consumenten antwoordt op deze mails en een bestelling plaatst, worden de oplichters nog steeds vlug miljonairs (de spammers nemen soms een winst van 900 tot 1000% op het verkochte product, dat zij oorspronkelijk hebben gekocht voor een bijzonder lage prijs in één of ander land dat gekend is voor zijn namaakproducten).

Voor de consument stelt de aankoop op internet van een nagemaakt product verschillende problemen. Het product stemt mogelijk niet overeen met hetgeen hem werd voorgesteld, het is niet erg betrouwbaar en is al vlug defect... zonder enige waarborg uiteraard ! Bovendien, heeft de consument geen recht op enige dienst na verkoop, daar de verkoper op het internet vaak niet identificeerbaar is.

Bovendien, is het mogelijk dat het nagemaakt product in beslag wordt genomen door de douane. De Europese verordening nr. 1383/2003 organiseert te dien einde een procedure die de douaneautoriteiten toelaat om, wanneer er voldoende redenen bestaan om te vermoeden dat men te maken heeft met goederen die een inbreuk uitmaken op een intellectueel eigendomsrecht, de goederen vast te houden om het de houder van het recht mogelijk te maken om een verzoek om optreden in te dienen.

Veel postpakken komen binnen via de Belgische luchthavens en worden verbeurd-verklaard door de douane die een – volkomen wettelijke – kloppacht houden op namaakproducten. De consument zou kunnen worden beschuldigd van heling en het is zeer waarschijnlijk dat hij de sommen, die hij oorspronkelijk heeft gestort, nooit zal terugzien ! De verkoper is immers vaak moeilijk te identificeren en is gevestigd in een ver land, hetgeen elke efficiënte vervolging onmogelijk maakt...

Wat de aankoop van namaakprogramma's betreft, zal de houder van de rechten op elk ogenblik een vordering uit hoofde van namaak kunnen instellen en u verbieden het programma – dat u hebt betaald aan de oplichter ! – te gebruiken.

Hij zal van een rechter, zelfs op eenzijdig verzoekschrift, de machtiging kunnen bekomen om over te gaan tot beslag inzake namaak door één of meerdere deskun-

digen (die worden benoemd door de rechter). De houder van de rechten kan aldus de beschrijving van alle voorwerpen en procédés bekomen waarvan wordt beweerd dat ze namaak zijn, u doen veroordelen tot betaling van een boete gaande van 100 tot 100.000 euro (te vermeerderen met de decimen, hetgeen concreet neerkomt op een vermenigvuldiging van dit bedrag met 5,5) indien u een kopie van een computerprogramma in het verkeer brengt of, voor commerciële doeleinden, in uw bezit hebt, wetende dat het gaat om een illegale kopie of redenen hebt om dit te geloven. In geval van herhaling, kan de boete van eenzelfde bedrag gepaard gaan met een gevangenisstraf van drie maanden tot twee jaar. De houder van de rechten zal eveneens de verbeurdverklaring van het programma (voorwerp van de inbreuk) kunnen bekomen en een eventuele schadevergoeding van u vorderen.

Wat de verkoop van valse diploma's betreft, gebeurt de productie ervan meestal in verre landen, hetgeen de vervolgingen niet gemakkelijk maakt, des te meer daar de afzender ook hier vaak moeilijk zal zijn te identificeren of te lokaliseren. Als een consument deze documenten echter gebruikt met de bedoeling om een potentiële werkgever te bedriegen, begaat hij een strafbare inbreuk (valsheid in geschrifte en/of gebruik ervan).

HOE HANDELEN ?

Al te goedkope aanbiedingen verbergen vaak namaakproducten of zelfs oplichtingen.

Meerdere aanwijzingen moeten de aandacht trekken op het risico bij de aankoop van dit soort producten :

- De prijs: een abnormaal lage prijs, die zelfs té interessant is, moet aanzetten tot voorzichtigheid en het vermoeden wekken dat het gaat om een namaakproduct ;
- De oorsprong van de aankoop : bepaalde gevoelige landen zijn gekend voor de namaak van luxeproducten ;
- De authenticiteitswaarborg : het certificaat dat samen met het product wordt geleverd, kan ook vervalst zijn en biedt dus geen enkele waarborg betreffende de legitimiteit van het product ;
- De verkoper : het gebrek aan precieze identificatie van de verkoper blijft verdacht (geen enkele bijzondere gegevens, behalve een e-mailadres dat niet veel waarborgt) ;
- De beschrijving van het product : bepaalde termen die gebruikt worden bij de beschrijving van het product – zoals kopie, replica, imitatie, ... – kunnen impliceren dat het gaat om namaak.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

In geval van twijfel, is het aangewezen om nooit te antwoorden op deze berichten en de voorgestelde producten niet te kopen... behalve indien u geld teveel hebt en geen gerechtelijke vervolgingen vreest !

VOOR MEER INFORMATIE

De website Consumentenbedrog : www.consumentenbedrog.be ;

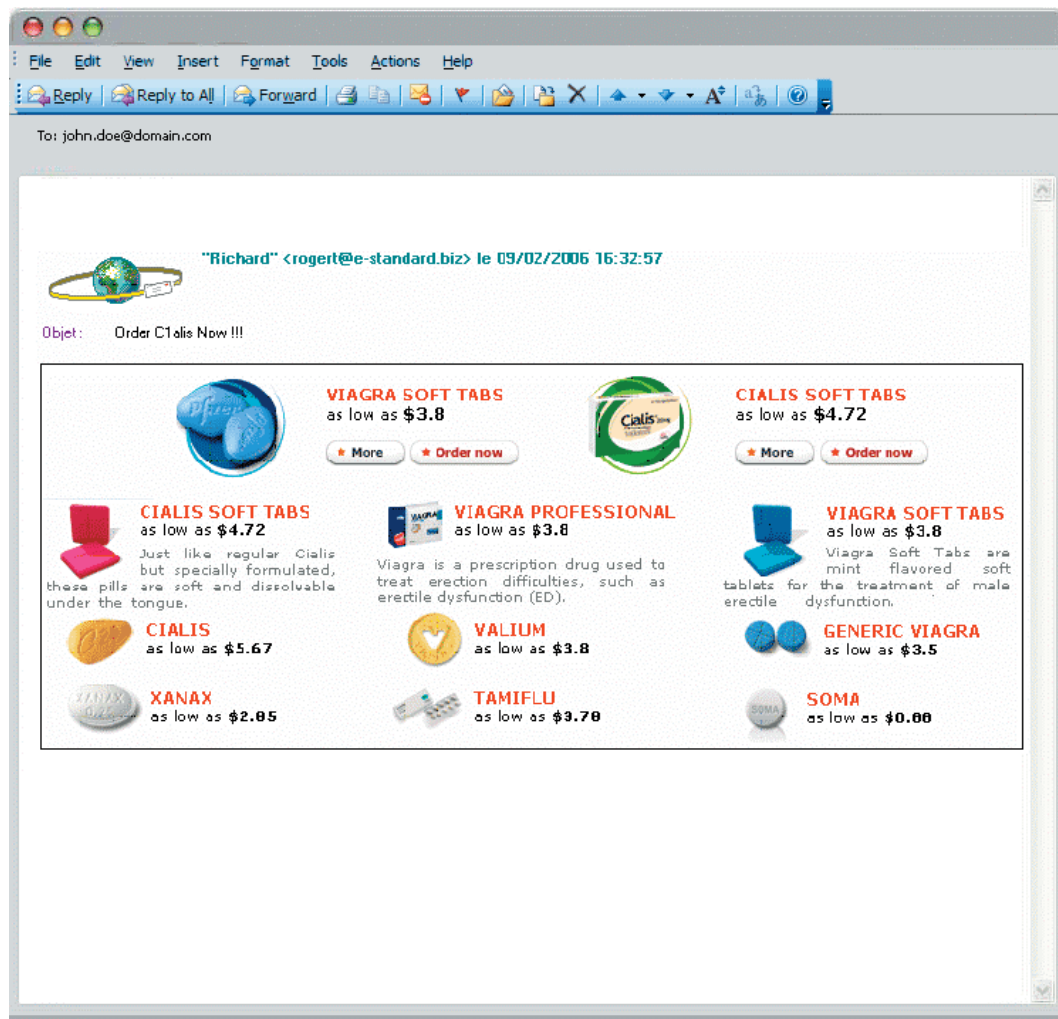
De website van de FOD Economie, KMO, Middenstand en Energie : www.economie.fgov.be, en in het bijzonder de rubriek inzake intellectuele eigendom : http://economie.fgov.be/intellectual_property/home_nl.htm ;

De website van de Administratie douane en accijnzen : www.fiscus.fgov.be/interfdafr/default.htm.

5. ELEKTRONISCHE BERICHTEN DIE WEINIG INZITTEN MET UW GEZONDHEID

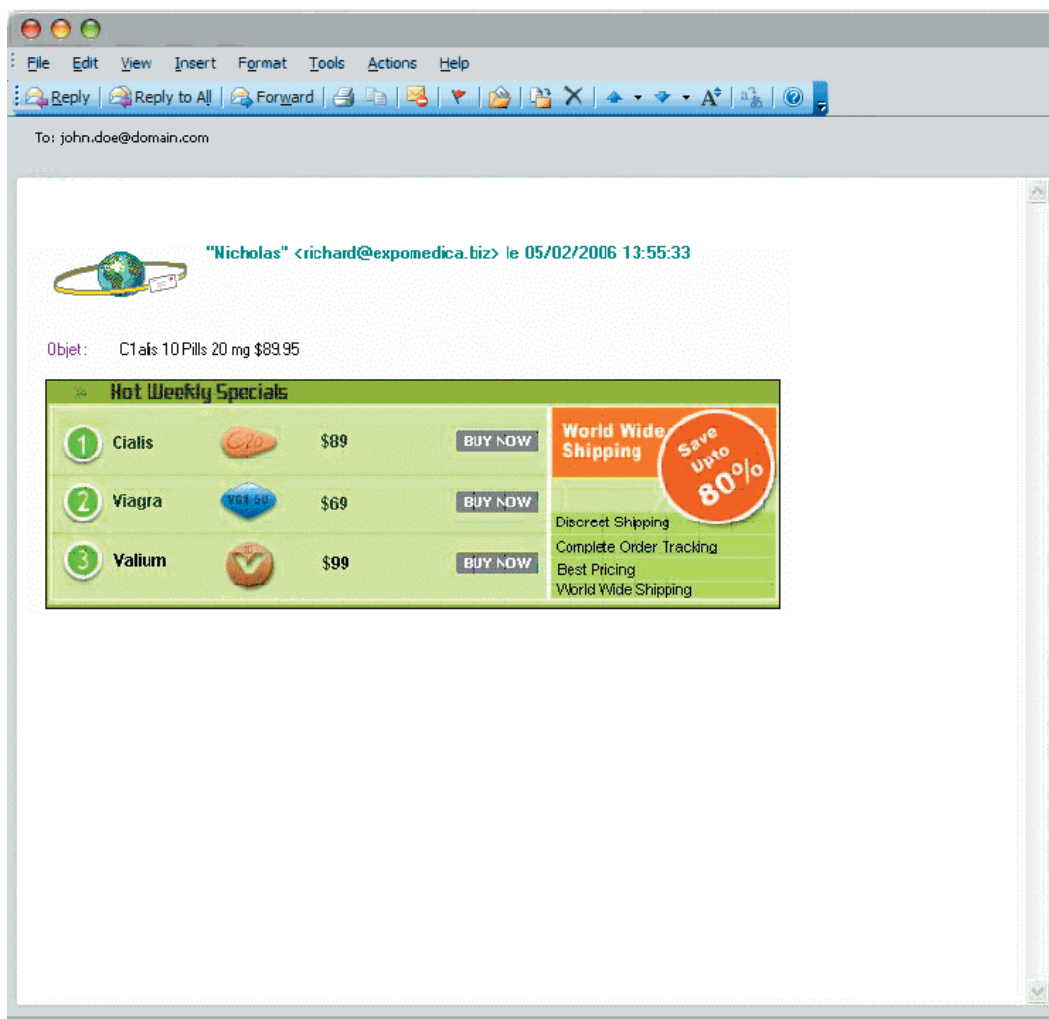
ILLUSTRATIES

Voorbeeld 1



« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Voorbeeld 2



UITLEG

Men ontvangt regelmatig e-mails met reclame voor gezondheidsproducten (sek-suele stimulans, vermageringsproducten, antidepressiva, enz.). Bovendien worden veel gezondheidsproducten te koop aangeboden op het internet.

Het is aangewezen om bijzonder voorzichtig te zijn ten aanzien van deze reclameberichten, die onwettelijk of bedrieglijk kunnen zijn en zelfs werkelijke gevallen van oplichting kunnen uitmaken die gevaarlijk kunnen zijn voor de gezondheid.

Er bestaan immers vele redenen waarom de aankoop van producten via internet een gevaar kan uitmaken voor uw gezondheid of, minstens, een ongemak of geldverlies kan vormen :

- De gebruiksaanwijzingen kunnen onbestaande, onjuist of onbegrijpelijk zijn (bijvoorbeeld in een taal die u niet kent) ;
- De distributiekanaalen voor de verkoop van gezondheidsproducten op internet zijn gewoonlijk niet de wettelijke circuits, die worden gecontroleerd door de bevoegde autoriteiten. In die omstandigheden, kunnen de kwaliteit van de producten, de omstandigheden van bewaring, de efficiëntie en de veiligheid ervan niet gewaarborgd worden. De aankoop van deze producten op het internet bevordert het risico op slecht gebruik, want deze producten zijn niet noodzakelijk aangepast of er kunnen tegenindicaties zijn ;
- De terugbetaling kan problemen stellen ;
- Het komt vaak voor dat men over geen enkele informatie beschikt over de verkoper en/of de fabrikant, hetgeen voor grote moeilijkheden zal zorgen indien u verduidelijkingen wenst over de kwalificaties van de verkoper of u, om de één of andere reden, tegen deze een vordering wil instellen ;
- Bepaalde producten die in het buitenland worden gekocht, zijn verboden in ons land. In geval van onwettelijkheid, kunnen uw producten in beslag worden genomen, verbeurdverklaard en zelf vernietigd door de douane, om het dan nog niet te hebben over de boete die u in dat geval verschuldigd zou zijn !

De grootste paradox is te moeten vaststellen dat de geneesmiddelen die op het internet worden verkocht, soms aan prijzen worden verkocht die (veel) hoger liggen dan diegene die in uw apotheek worden gehanteerd ! Wij herinneren er hier aan dat de prijs van geneesmiddelen gereguleerd is in België en dat het terugbetalingsstelsel, dat in ons land bestaat, vaak interessant is voor de patiënt.

HOE HANDELEN ?

Voorzichtigheid is geboden wanneer u beslist om producten betreffende uw gezondheid te kopen via het internet. In vele landen, kan de procedure van aankoop van geneesmiddelen via het internet zelfs onwettelijk zijn. Wij kunnen u dus slechts aanraden om geneesmiddelen en andere gezondheidsproducten via de wettelijke distributiekanaalen aan te kopen, zoals bv. in de apotheken wat geneesmiddelen betreft.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Speel niet voor leerling-tovenaar ! Door gezondheidsproducten te bestellen via internet, neemt u mogelijk risico's voor uw gezondheid en voor uw portefeuille en, vooral, ontnemt u uzelf soms de mogelijkheid om te genieten van duidelijke adviezen en raad van uw dokter, apotheker of andere persoon werkzaam in de gezondheidssector.

De Algemene Directie Geneesmiddelen van de FOD Volksgezondheid publiceert regelmatig waarschuwingen betreffende de verkoop van gezondheidsproducten op het internet op het volgende adres: www.health.fgov.be (raadpleeg de rubriek « Geneesmiddelen »). **Wij nodigen u uit om deze website regelmatig te bezoeken.**

Dezelfde Algemene Directie strijdt tegen de illegale reclame en verkoop van geneesmiddelen en medische hulpmiddelen op het internet, o.m. in samenwerking met de FOD Economie en andere nationale en internationale instanties.

Om aan de AD Geneesmiddelen de gevallen van activiteiten over te maken die zij vermoeden illegaal te zijn, alsook de probleemgevallen betreffende gezondheidsproducten, kunnen de internetgebruikers op het volgende adres terecht :

FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu
Algemene Directie Geneesmiddelen
Bischoffsheimlaan 33
B-1000 Brussel
Tel : + 32 (0)2 227 55 25
Fax : + 32 (0)2 227 56 46
E-mail : info.dgm@health.fgov.be

VOOR MEER INFORMATIE

Wij raden aan om de « **Gids Geneesmiddelen en Internet** » te raadplegen. Deze gids werd opgesteld op initiatief van de Wereldgezondheidsorganisatie (WHO) en is beschikbaar op de website van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu : www.health.fgov.be (raadpleeg de rubriek « Geneesmiddelen », subrubriek « Geneesmiddelen en Internet »).

De waarschuwingsberichten van de AD Geneesmiddelen betreffende de verkoop van gezondheidsproducten op internet worden verspreid op de site www.health.fgov.be (raadpleeg de rubriek « Geneesmiddelen »). Wij nodigen u uit om deze website regelmatig te bezoeken.

Voor aanvullende informatie over oplichting m.b.t. de gezondheid, verwijzen wij de lezer ook naar de rubriek « Consumentenbedrog in de gezondheidssector », beschikbaar op de website www.consumentenbedrog.be van het OIVO (Onderzoeks- en Informatiecentrum van de Verbruikersorganisaties).

6. ELEKTRONISCHE BERICHTEN DIE INFORMATICA-VIRUSSEN VERSPREIDEN

ILLUSTRATIE

Gelet op de grote verscheidenheid van virussen die per e-mail kunnen verzonden worden, is het moeilijk om dit fenomeen te illustreren. In de praktijk, komt het erg vaak voor dat deze virussen zich bevinden in bestanden in bijlage van de e-mail. Wees dus voorzichtig bij het openen van deze bestanden! U vindt op de gespecialiseerde sites (zie « Voor meer informatie » hieronder) de verschillende virussen die per e-mail verzonden worden, de gevolgen ervan, hun schadelijk karakter en de wijze om deze virussen te vermijden of zich ervan te ontdoen.

UITLEG

36

Het doel van deze brochure is niet om een inventaris op te maken van de verschillende vormen van informatica-virussen, van hun gevaarlijkheid en van de oplossingen om ze te vermijden of te bestrijden. Betreffende deze verschillende vragen, verwijzen wij de lezer naar de brochure « Praktische fiches voor beveiliging » beschikbaar op het volgende adres : www.spamsquad.be.

Duidelijkheidshalve, beperken wij ons tot het verstrekken van de volgende informatie.

U dient er zich bewust van te zijn dat e-mail vaak wordt gebruikt door oplichters of hackers om informatica-virussen te laten rondgaan. Het gaat om min of meer schadelijke computerprogramma's die uw informaticasysteem kunnen besmetten.

Aldus, pogen hackers o.m. vanop afstand de controle te verwerven over uw computer en deze te sturen of u informaticamodules toe te sturen die het gebruik van de dienst beperken ofwel het netwerk of uw computer verlammen en zelfs beschadigen (bijvoorbeeld, door gegevens te vernietigen).

Er bestaat een grote verscheidenheid aan virussen, zonder de nieuwe te tellen die er elke dag bijkomen. Specialisten klasseren ze volgens hun verspreidings- en besmettingswijze :

- **Wormen** zijn virussen die zich langs een netwerk kunnen verspreiden ;
- **Trojaanse paarden** (malwares, spywares, dialer, enz.) zijn virussen die een fout kunnen veroorzaken in uw informaticasysteem. Deze worden over het alge-

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

meen in het geniep geïnstalleerd door een hacker om hem de mogelijkheid te geven om een computer van op afstand te controleren, om toegang te krijgen tot de inhoud ervan of om kennis te nemen van geheime informatie die wordt verstrekt tijdens een transactie (paswoord, nummer van kredietkaart, enz.) of nog, om gebruik te maken van de verbinding van de modem van de surfer om verbinding te maken met een vaak buitenlandse site met hoge facturatietarieven ;

- **Logische bommen** zijn virussen die in werking kunnen worden gesteld n.a.v. een bepaald evenement (datum van het systeem, activering van op afstand, ...) ;
- Een **hoax** is een fopbericht dat u ertoe aanzet om een waarschuwing te sturen naar al uw contacten, hetgeen leidt tot een verstopping van de netwerken en tot desinformatie (zie infra).

In dezelfde lijn, zonder dat men dit programma als een virus kan beschouwen, gebruiken de oplichters soms een « veiligheidsscanner ». Het gaat om een hulpmiddel waarmee men een veiligheidsaudit kan uitvoeren op een netwerk door de open poorten op een machine te analyseren om de risico's op het gebied van veiligheid te bepalen.

Dit werkmiddel is uiteraard zeer nuttig voor de systeem- en netwerkadministratoren om te waken over de veiligheid van het informaticapark waarmee zij belast zijn. De keerzijde van de medaille is dat dit werkmiddel soms gebruikt wordt door hackers om de gaten in het systeem te ontdekken en de open en onbewaakte poorten van de computer op te sporen.

HOE HANDELEN ?

Laten we maar meteen opmerken dat de lezer veel gedetailleerde raadgevingen over de efficiëntste manier om zijn informaticasysteem te beveiligen en aldus virussen en andere schadeverwekkende aanvallen te vermijden, kan vinden in de « Praktische fiches voor beveiliging », beschikbaar op het volgende adres : www.spamsquad.be.

Wij herhalen desalniettemin enkele elementaire preventieve maatregelen die het risico op een aanval en op de infectie door virussen zouden moeten verminderen.

1. Installeer een firewall (d.i. een programma dat uw computer beschermt tegen indringing komende van het internet) en een anti-virusprogramma (maar ook anti-spyware/mal-ware), update deze zo vaak mogelijk en voer regelmatig een volledige analyse uit van uw harde schijf(ven). **OPGELET** : een firewall is nutteloos zonder installatie van een anti-virusprogramma en omgekeerd !

2. Update regelmatig de verschillende programma's die zijn geïnstalleerd op uw computer (exploitatiesysteem, messaging, enz.) en installeer eventuele herstellingssystemen (patches) voor de bugs of fouten voor de versie van uw programma ;
3. Open geen bestand in bijlage van een e-mail, zeker niet als het uitvoerbaar is (.exe), of een link die u via e-mail ontvangt als u niet zeker bent van de authenticiteit ervan, vooral als deze e-mail aangeeft dat hij een oplossing bevat om uw computer te beschermen ;
4. Maak regelmatig een back-up van uw gegevens.

Om dagelijks geïnformeerd te worden over nieuwe virussen die verschijnen op het internet, kan de surfer zich abonneren op een verspreidingslijst die de alarmmeldingen van het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) verspreidt en/of websites raadplegen die gespecialiseerd zijn op dit vlak.

VOOR MEER INFORMATIE

38

« Praktische fiches voor beveiliging » verkrijgbaar op het volgende adres :
www.spamsquad.be ;

Rubriek « Consumentenbedrog m.b.t. computers en netwerken » van de website :
www.consumentenbedrog.be ;

De rubriek « virus info » van het BIPT : www.bipt.be/virus/viruswarning.htm ;

De rubriek « virus » van de website www.hoaxbuster.com ;

Gespecialiseerde site inzake virussen : www.secuser.com (in het Frans) ;
www.insecure.org (in het Engels) ; www.securityfocus.com (in het Engels) ;

Website van de Amerikaanse regering : <http://onguardonline.gov/spyware.html> (in het Engels).

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

7. ELEKTRONISCHE BERICHTEN DIE DE KLASSIEKE GEVALLEN VAN OPLICHTING BEHELZEN

ILLUSTRATIE

Jammer genoeg zijn wij – de oplichterijen – te talrijk om in dit document te kunnen worden geïllustreerd. Kom ons dus bezoeken en ons leren herkennen op de hieronder vermelde gespecialiseerde websites (zie « Voor meer informatie »).

UITLEG

Wiens aandacht werd nooit getrokken door de mooie beloftes van een reclame waarin schoonheid, prestaties, geluk worden aangeprezen? Vandaag de dag is oplichterij meer dan ooit een internationaal fenomeen. Oplichters gebruiken de nieuwe technologieën met een indrukwekkend professionalisme.

Oplichters hebben uiteraard de komst van het internet niet afgewacht om hun wanpraktijken te beoefenen.

Het gebruik van e-mail (alook, zoals men steeds vaker ziet, het gebruik van instant messaging of van blogs) houdt echter onmiskenbare troeven in vergelijking met de gevallen van oplichting die worden gepleegd in de straat, per telefoon, per fax of per brief: de kost, de snelheid en het aantal potentiële slachtoffers dat ermee kan bereikt worden (duizenden in enkele seconden!).

In deze context, bestaat er geen twijfel over dat e-mail het medium bij uitstek is geworden om misdrijven te plegen!

Via e-mail, pogen oplichters hun slachtoffers – soms aanzienlijke – geldsommen te ontfutselen alvorens in rook op te gaan zonder enig spoor achter te laten. De Algemene Directie van Controle en Bemiddeling van de FOD Economie en de Federale Politie worden elke dag geconfronteerd met slachtoffers die schade hebben geleden die zeer belangrijk kan zijn.

Deze gevallen van oplichting zijn erg talrijk en kunnen varianten voorstellen en kunnen zich zowel in een elektronische als een niet-elektronische context ontwikkelen. Het doel van deze brochure is niet om een volledige inventaris te geven van deze vele gevallen van oplichting. Wij verwijzen de lezer naar bepaalde referentiewebsites die zeer volledig zijn en regelmatig worden geüpdate (zie de rubriek « Voor meer informatie » hieronder).

Om de variëteit te illustreren, beperken wij ons tot het citeren van de naam van enkele vaak voorkomende gevallen van oplichting die in een lijst zijn opgenomen :

- Identiteitsfraude ;
- Voorstellen die te mooi zijn om waar te zijn (Nigeriaanse brieven, valse loterijen, herverkoop van time-sharing, piramideverkoop, verkoop van tafelgarnituur, reclame voor thuiswerk, mirakelproducten, reizen aan spotprijzen, ...) ;
- Gedwongen downloaden van verbindingsoftware naar een duur telefoonnummer (« dialer ») of aanbod van valse diensten via een duur telefoonnummer ;
- Valse beweringen betreffende de gezondheid ;
- Oplichting inzake huwelijk en dating ;
- Aanbod van valse of dwaze diensten (helderziende, medium, enz.) ;
- Valse verkoop of koop met vervalste cheques ;
- Valse verzoeken tot giften (vaak ten gevolge van dramatische gebeurtenissen zoals de tsunami in Azië of Katrina) ;
- Enz.

HOE HANDELEN ?

De beste raad die we u kunnen geven om gepast op deze pogingen tot oplichting te reageren en om te vermijden dat u in de val trapt, is de volgende : informeer u !

Neem de tijd om het voorstel dat u wordt gedaan te analyseren. Leer de verschillende types van oplichting te herkennen en leer de eenvoudige methodes om erop te reageren voor het te laat is.

Om dit te doen, kunnen wij u slechts uitnodigen om de gespecialiseerde en geüpdate sites te raadplegen die uitleg geven over talloze gevallen van oplichting om na te gaan of het voorstel niet overeenstemt met één van de casussen. Wij raden in het bijzonder de volgende officiële websites aan :

- De FOD Economie :
www.economie.fgov.be/protection_consumer/fraud_prevention/home_nl.htm ;
- De « Federal Computer Crime Unit » van de Federale Politie :
www.fccu.be/crim/crim_fccu_fr.php ;
- De website « Consumentenbedrog » van het Onderzoeks- en Informatiecentrum van de Verbruikersorganisaties (OIVO) : www.consumentenbedrog.be.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Indien uw twijfels bevestigd worden n.a.v. de raadpleging van deze informatiebronnen, reageer dan niet en verwijder de e-mail. Indien u toch nog zou twijfelen, neem dan contact op met de Algemene Directie Controle en Bemiddeling van de FOD Economie (eco.inspe@economie.fgov.be) of met een consumentenorganisatie om oordeelkundige raad te verkrijgen.

Een verwittigd mens is er twee waard !

VOOR MEER INFORMATIE

De website van de FOD Economie : http://economie.fgov.be/protection_consumer/fraud_prevention/home_nl.htm ;

De website van de FCCU (Federale Politie) : www.fccu.be/crim/crim_fccu_fr.php ;

De website « Consumentenbedrog » van het OIVO: www.consumentenbedrog.be ;

De verwittigde cyberconsument : www.clcv.org ;

De website www.hoaxbuster.com ;

Andere websites over oplichting : www.lesarnaques.com, www.scambusters.org.

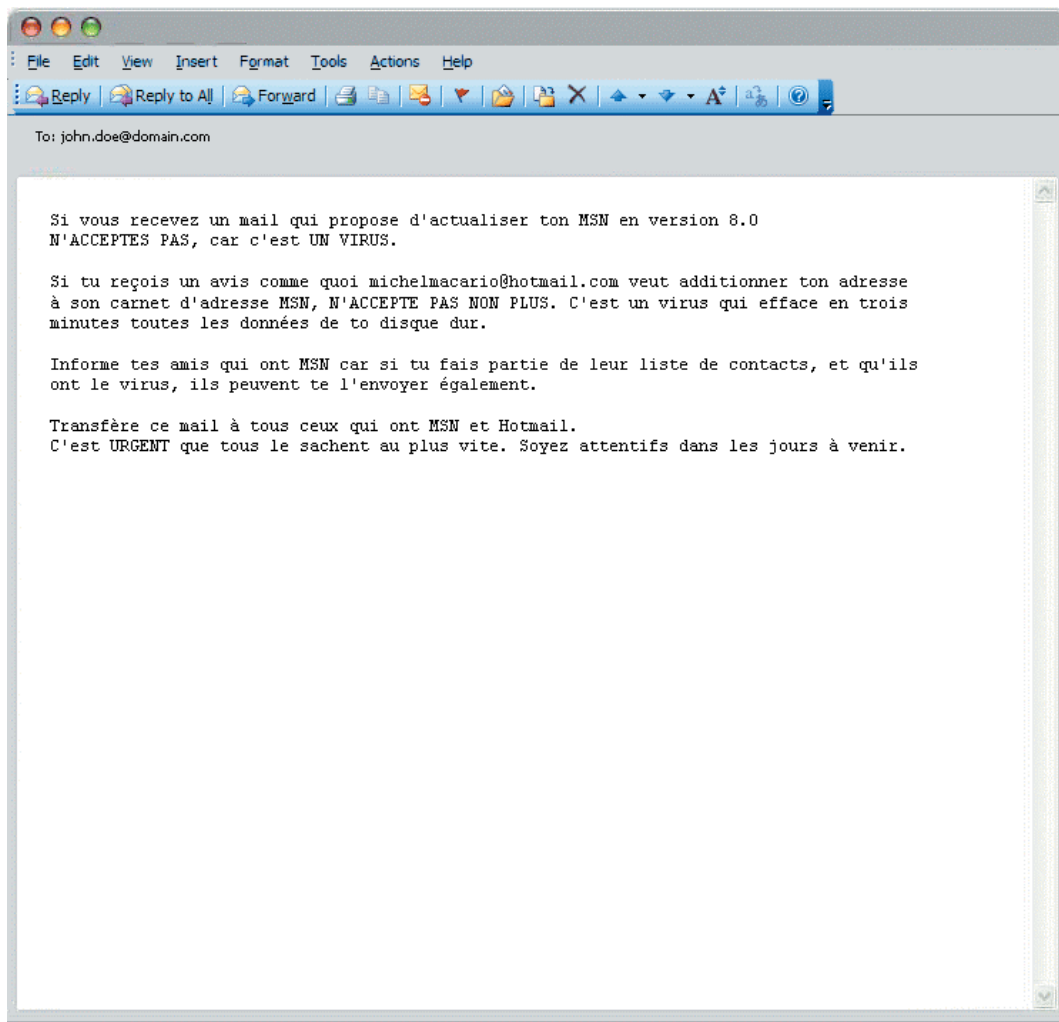
« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

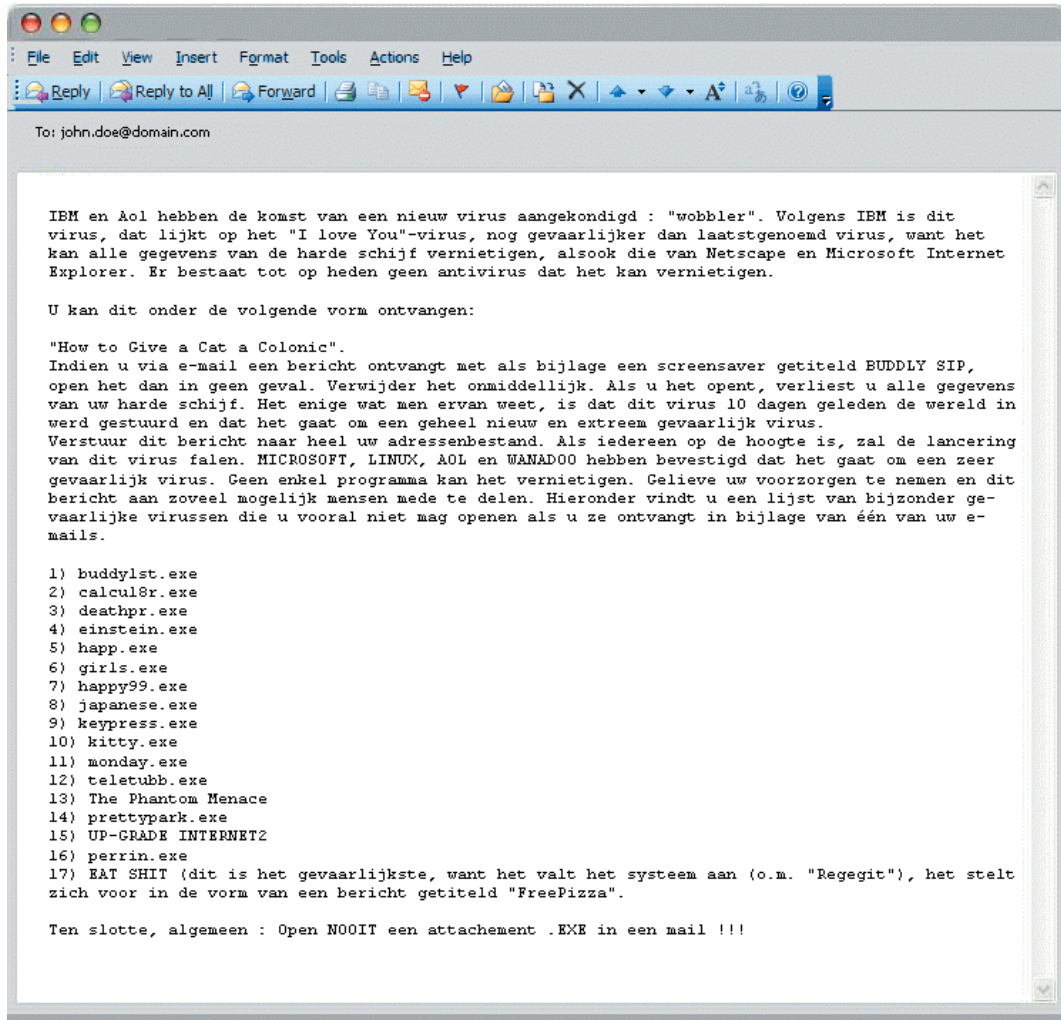
DEEL 2 : ONGEVRAAGDE ELEKTRONISCHE BE- RICHTEN MET BEPERKTE GEVAARLIJKHEIDS- GRAAD

1. DE « HOAX », FOPBERICHTEN OF GERUCHTEN

ILLUSTRATIES

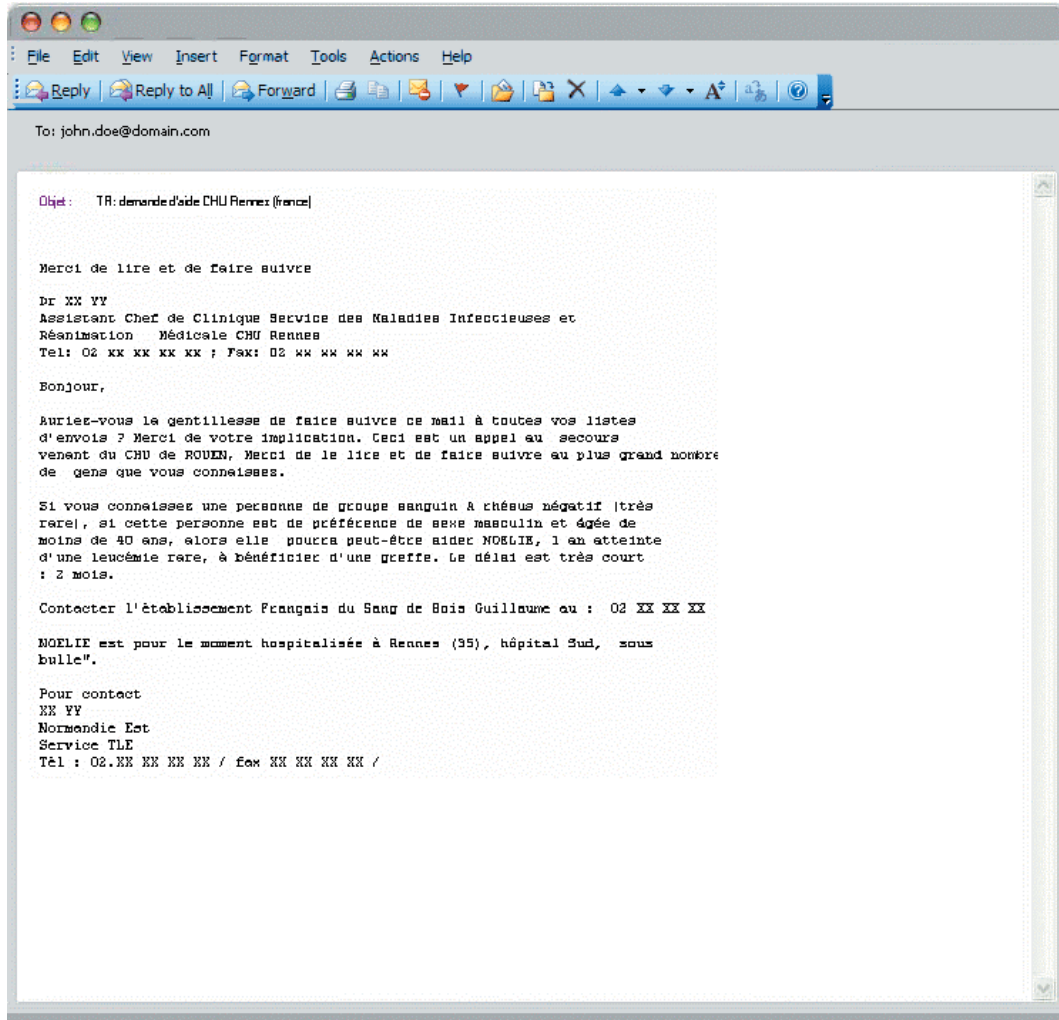
Voorbeeld 1 : valse virussen



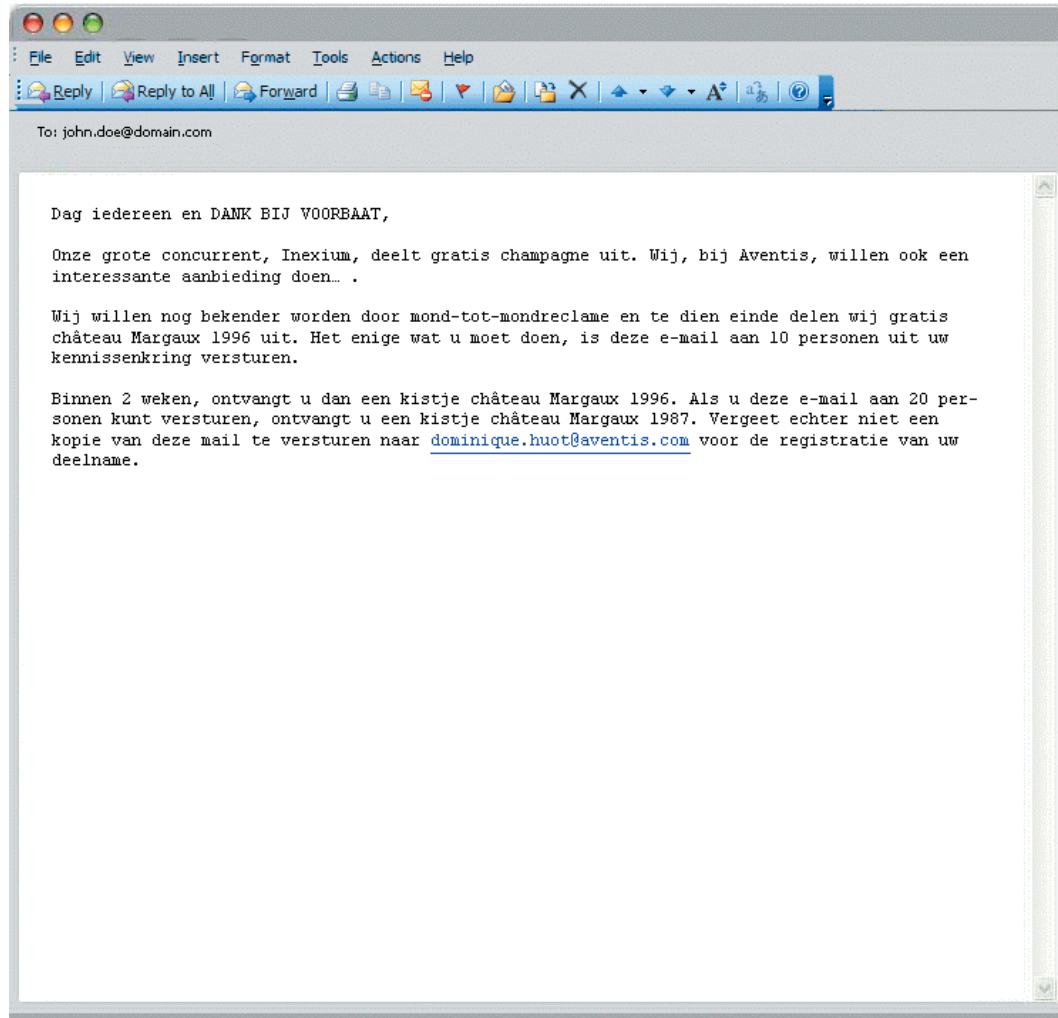


« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Voorbeeld 2 : de solidariteitsketting

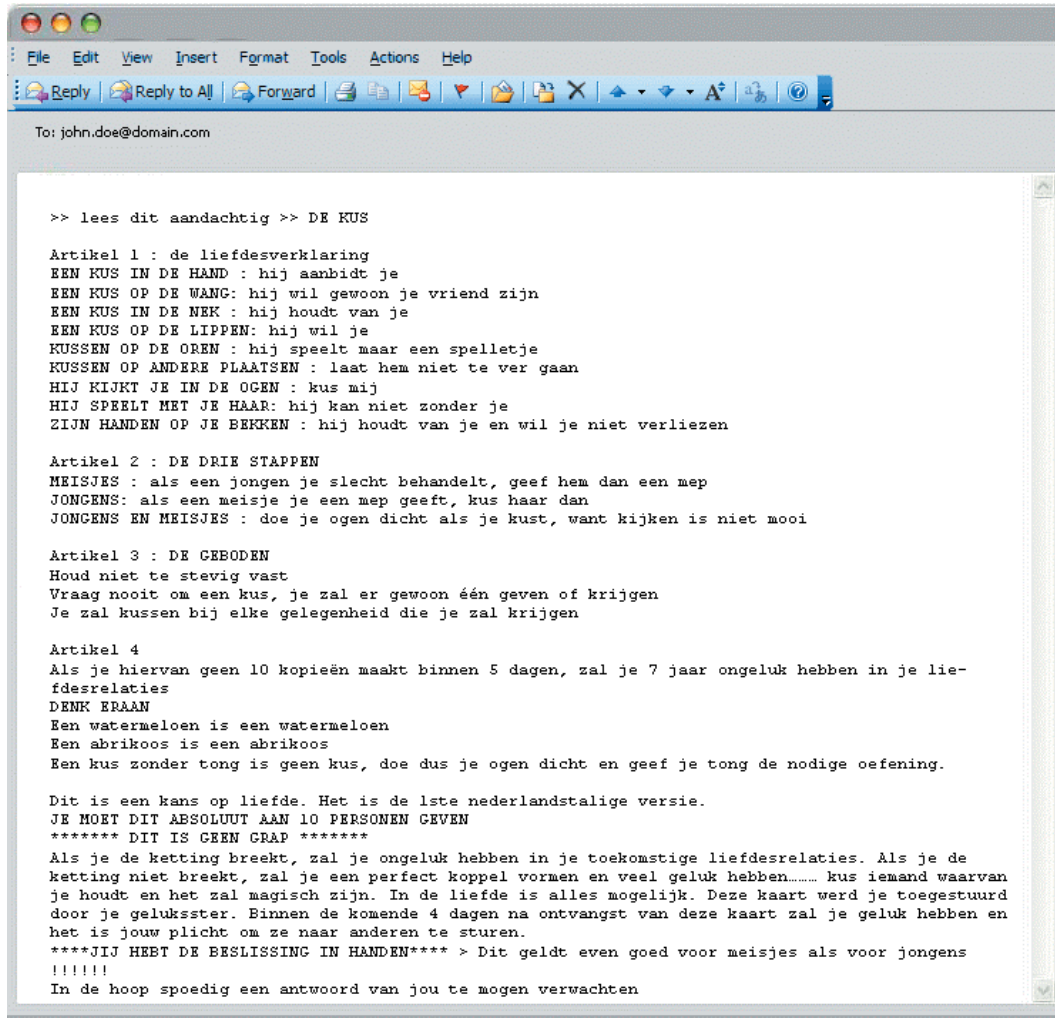


Voorbeeld 3 : belofte van « winsten » of gratis producten

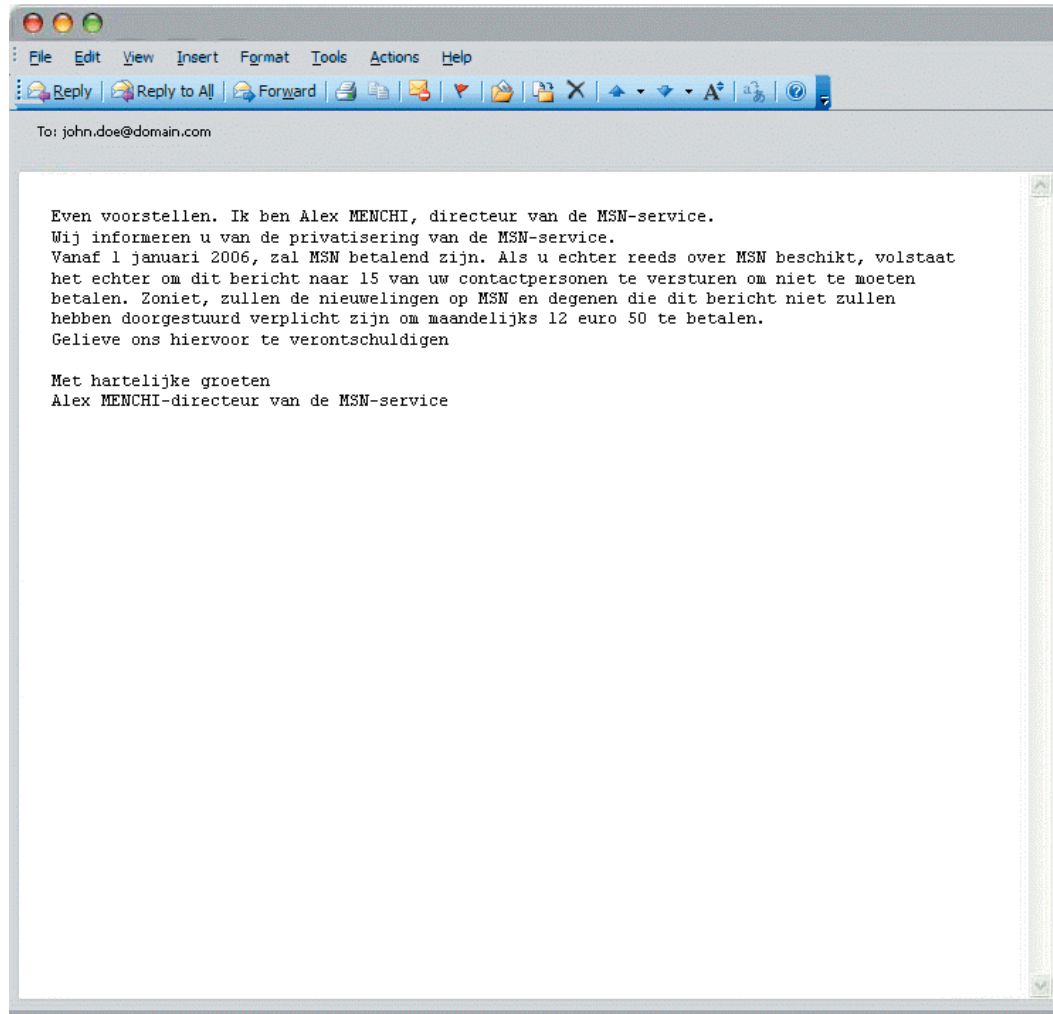


« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

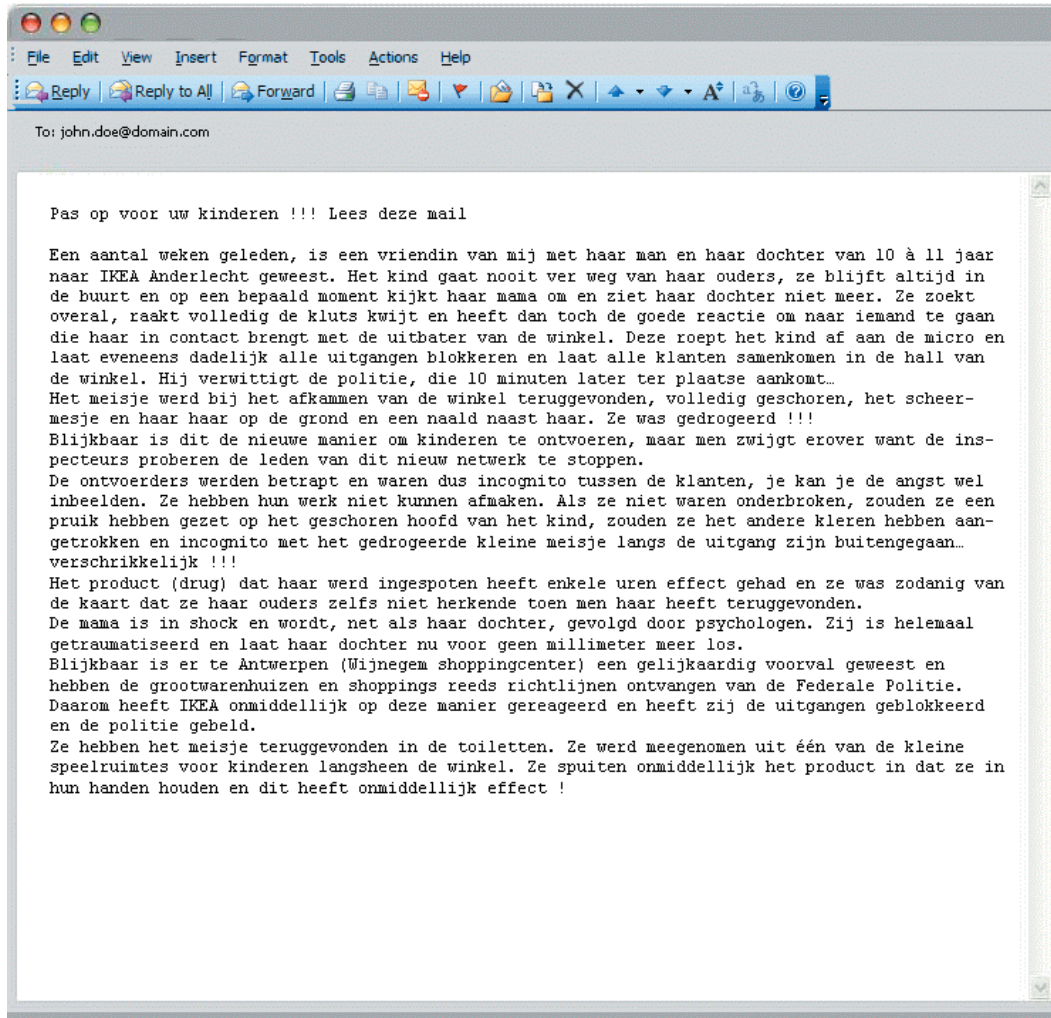
Voorbeeld 4 : geluk of ongeluk



Voorbeeld 5 : foute informatie of vals gerucht

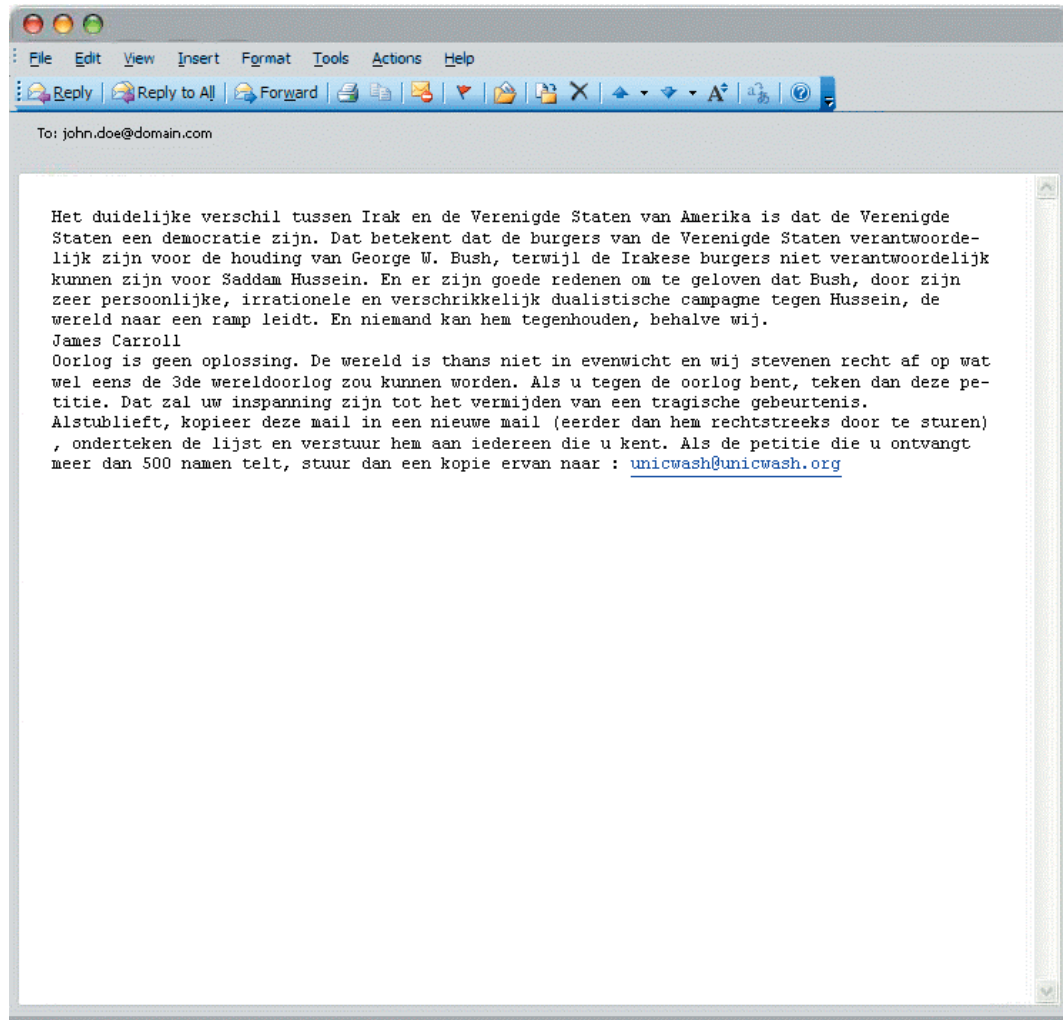


« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »



Ten gevolge van het rondgaan van deze e-mail, heeft IKEA (en meer bepaald de Belgische winkel te Anderlecht) snel gereageerd en een communiqué laten rondgaan waarin de informatie zeer duidelijk wordt ontkend.

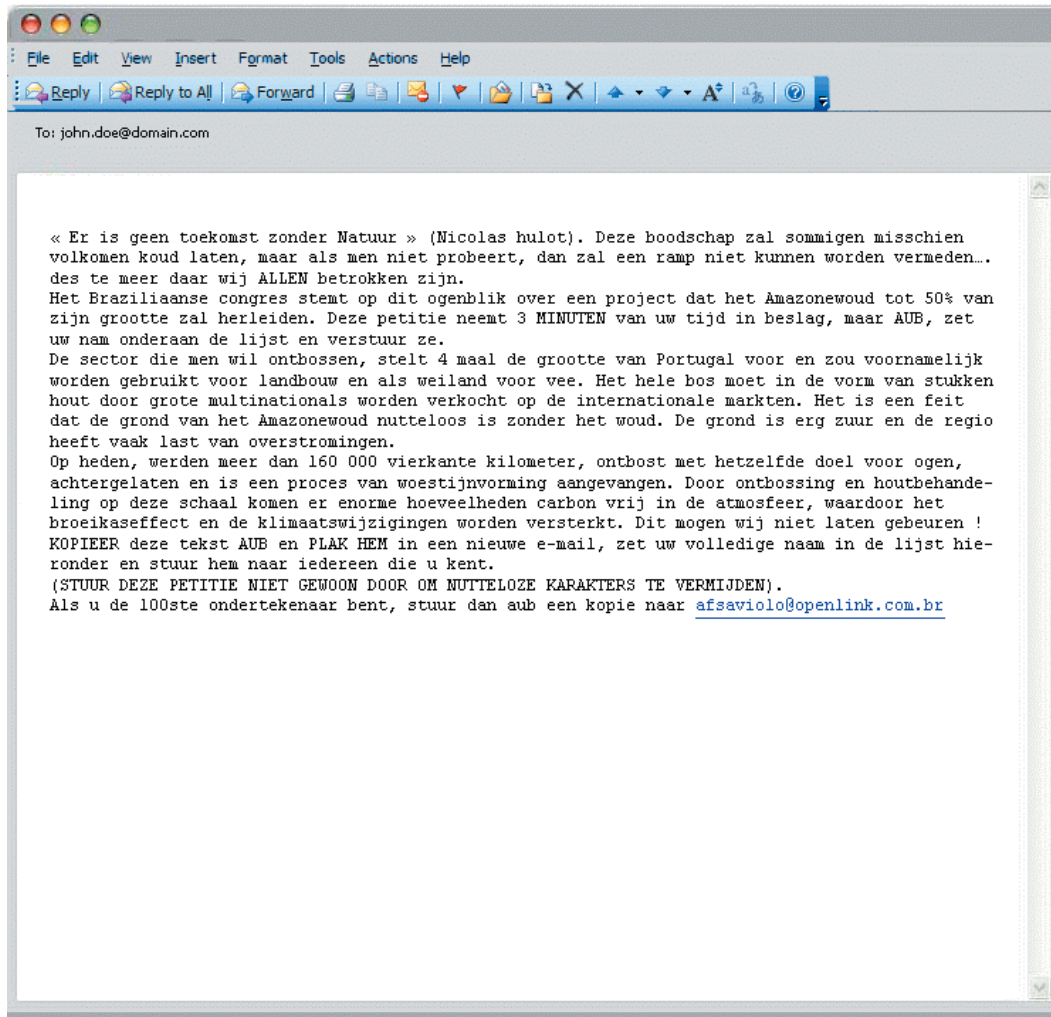
Voorbeeld 6 : de valse petitie tegen de oorlog in Irak



Deze petitie is een fopbericht en het informatiecentrum van de Verenigde Naties ("the United Nations Information Centre") te Washington (<http://unicwash.org>), heeft met deze hele zaak niets te maken. Het heeft dan ook geen zin ernaar te schrijven.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Voorbeeld 7 : de valse petitie van Nicolas HULOT, verzonden per e-mail



51

De stichting Nicolas Hulot bestaat echt en doet concrete acties in verband met het milieu. De verantwoordelijken van deze stichting verduidelijken echter dat "deze petitie uiteraard niet uitgaat van Nicolas Hulot, noch van de Stichting Nicolas Hulot".

UITLEG

Wie heeft nog nooit een « hoax », ook fopbericht genoemd, op zijn e-mailadres ontvangen ?

Sinds mensenheugenis, verheugen fopberichten de consument. Eerst nog via de post of per telefoon, thans hebben zij met de komst van het internet en e-mail mondiale dimensies aangenomen. Los van grenzen, afstand, tijd en kosten komen zij rechtstreeks en gemakkelijk in uw inbox terecht.

Bovendien kunnen ze verschillende vormen aannemen, o.m. die van virusalarmen, valse solidariteitskettingen, valse petitie's, valse belofte's, valse informatie, grapjes met een vreemde smaak, ...

Dit bericht, dat meestal wordt verzonden door een vriend, wordt vaak als dringend bestempeld. De eerste reflex bestaat er dan ook uit om dit alarmbericht zo snel mogelijk naar al uw kennissen te versturen. Laatstgenoemden doen dan exact hetzelfde enzovoort totdat, door een « sneeuwbal-effect », het bericht meermaals om de wereld gaat !

Het probleem is dat dergelijke « hoax » een beroep doet op uw naïveteit en bepaalde gevaren kan inhouden. Om deze reden, willen wij hier uw aandacht trekken op de kenmerken waaraan u een « hoax » kan onderscheiden van een legitiem bericht, de verschillende types van meest voorkomende « hoax » en ten slotte de gevaren die deze berichten inhouden.

Kenmerken van een « hoax »

Een fopbericht of een hoax heeft meestal de volgende, makkelijk herkenbare kenmerken :

- Het bericht is gericht aan een lijst van correspondenten en niet aan één enkele bestemming ;
- Het bericht is intrigerend, onrustwekkend of zelfs choquerend van aard ;
- Daar het bericht de lezer niet ongevoelig laat, weekt het een reactie bij deze los ;
- De informatie wordt gewaarborgd door betrouwbare referenties, die echter nooit worden bewezen ;
- De surfer wordt uitgenodigd om het bericht door te sturen naar zijn kennissen ;
- Het bericht bevat vaak spel- of syntaxisfouten.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Meest voorkomende types van hoax

De meest voorkomende types van hoax zijn de volgende (deze lijst is opgenomen op de website www.hoaxbuster.com) :

1/ VALSE VIRUSSEN

Het bericht – dat wordt geacht te komen van grote vennootschappen (IBM, AOL, Microsoft, ...) – waarschuwt u voor de bliksemsnelle verspreiding van een virus via e-mail. Het bericht moedigt u aan om een zo groot mogelijk aantal personen te verwittigen, gelet op de hoogdringendheid van de situatie en op het gevaar van het virus. Het bericht wordt soms ondertekend door hoge informaticaverantwoordelijken of door hoog aangeschreven persagentschappen.

In werkelijkheid, zijn veel van dit soort berichten eenvoudigweg vals. In geval van twijfel heeft de surfer er belang bij om de informatie te controleren op gespecialiseerde websites zoals www.secuser.com of www.hoaxbuster.com.

53

2/ SOLIDARITEITSKETTINGEN

Dit type van bericht doet een beroep op de gulheid van de surfers. Het bericht moedigt u immers aan tot het redden van één of meerdere personen (die lijdt/lijden aan een ernstige ziekte, enz.). Men deelt u mede dat de internet providers geacht worden al uw berichten te tellen en in functie daarvan een bepaalde som over te maken aan de ongelukkige(n). Kort gezegd, men zet u ertoe aan om zoveel mogelijk berichten te versturen, daar hoe vaker het bericht wordt verzonden, des te meer geld de beweerde ongelukkige zal ontvangen.

U zal echter vaststellen dat de operatie door geen enkele sponsor wordt gesteund, dat het bericht geen enkele link bevat naar een partner (een officiële organisatie) en, ten slotte, dat de e-mailadressen, als ze zichtbaar zijn, allemaal vals zijn. En terecht: de beweerde ziekte bestaat niet en de persoon die eraan lijdt nog minder !

3/ BELOFTE VAN « WINSTEN » OF VAN GRATIS PRODUCTEN

Het bericht dat u belooft om in geen tijd een grote som geld te winnen. Daarvoor volstaat het om het bericht naar zoveel mogelijk personen te sturen. Een programma wordt geacht uw verzendingen te tellen. Het gebeurt zelfs dat het bericht wordt gestaafd aan de hand van een (verbijsterend) voorbeeld dat u aantoont hoe u aldus vele duizenden dollars kan winnen !

Het gebeurt ook dat de berichten worden verzonden in naam van een gekende onderneming en dat deze vermelden dat men een gratis product kan ontvangen als men het bericht aan X aantal mensen verstuurt, alsook aan een verantwoordelijke van de onderneming in kwestie, waarvan het e-mailadres wordt vermeld.

Er heeft nog nooit iemand geld verdiend door eenvoudigweg een e-mail te versturen. Het beste bewijs ervan is dat niemand ooit de gelukkige winnaar van deze actie heeft gekend... En bovendien, als het waar zou zijn, dan zou het geweten zijn !

4/ GELUK OF ONGELUK

Iedereen heeft al wel eens een dergelijke brief ontvangen. Het bericht wijst u aan als gelukkige bestemming van het grote geluk of van het verschrikkelijkste ongeluk naargelang u het bericht doorstuurt of niet (soms wordt ook een aantal personen aangeduid).

Om het bericht kracht bij te zetten, citeert men het voorbeeld van een persoon die het bericht niet doorgestuurd heeft en die al het ongeluk van de wereld op zijn hoofd heeft gekregen totdat hij uiteindelijk van gedacht veranderde, waarna al zijn problemen plots verholpen waren.

Bijgeloof zet sommige mensen er weliswaar soms toe aan om het bericht door te sturen. Maar moet de rede het niet altijd halen van het bijgeloof ? Verwijder het bericht en verleng de ketting vooral niet.

5/ DESINFORMATIE

Het bericht "informeert" de surfer van het één of ander feit. Het feit in kwestie kan schandalig zijn (bijvoorbeeld deze of gene hoog aangeschreven vennootschap werkt samen met een rechts-extremistische partij). Het kan ook verontrustend zijn (een kind wordt bijvoorbeeld op een spectaculaire manier ontvoerd in een bekend grootwarenhuis). Het kan ten slotte dringend zijn (bijvoorbeeld hernieuwing van het rijbewijs binnen een bepaalde termijn om het gratis te kunnen bekomen).

Het aangehaalde feit is over het algemeen van die aard om de surfer te doen reageren, hetgeen het beoogde doel is. Over het algemeen worden zeer bekende vennootschappen erbij betrokken en zoekt het bericht een verspreiding op grote schaal van het schandaal, van de onrustwekkende of dringende informatie.

Naast het feit dat de informatie vals is, is de ondertekenaar van het bericht wel te verstaan onbekend. Daarentegen, komt het vaak voor dat personen die hierdoor in een kwaad daglicht worden gesteld, wel echt bestaan. In het laatste geval, maakt het fopbericht laster uit.

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

6/ TWIJFELACHTIGE PETITIES

Door zijn snelheid, is e-mail een vaak gebruikt middel voor petities, maar niet altijd zonder gevaar. Overeenkomstig ons Belgisch devies « eenheid maakt macht », stelt dit soort van bericht voor aan de surfers om zich te verenigen tegen het onrecht. De surfer wordt aldus uitgenodigd om zijn naam in te schrijven op een lijst, na andere ondertekenaars, om tegen dit onrecht te protesteren.

Het gebrek aan identificatie van de opdrachtgevende vereniging en van de persoon aan de basis van de petitie moet echter de aandacht trekken. Want een e-mail ondertekenen en hem versturen naar kennissen is hetzelfde als een fles in de zee werpen zonder enige waarborg.

De petitie zal immers gewoon de wereld rondgaan zonder meer indien niemand de opdracht krijgt om ze over te maken aan de bestemming (het is zelfs mogelijk dat het adres dat wordt opgegeven als zijnde dat van de bestemming al lange tijd niet meer actief is). Om nog maar te zwijgen over het feit dat, op om het even welk moment, om het even welke surfer de inhoud van de oorspronkelijke tekst kan veranderen en andere ideeën kan versturen met de « onvrijwillige » steun van de voorgaande ondertekenaar.

De ondertekening van een petitie is een daad die de burger verbindt. Om die reden is het beter om de kwaliteit van de voorgestelde inhoud te controleren, alsook de legitimiteit van de afzender ervan en petities te gebruiken die men terugvindt op een site waar de initiatiefnemer en de bestemming zijn geïdentificeerd en waar de informatie kan gecontroleerd.

7/ HUMOR

Humoristische berichten, die men vaak per toeval via e-mail ontvangt, laten niemand ooit ongevoelig. Dergelijke e-mails worden gekenmerkt door een gebrek aan ondertekening en het feit dat ze op universele wijze alle surfers betrekken. Surfers, die op zoek zijn naar ontspanning, nemen deze mail over en besmetten aldus andere surfers in de hoop hen een plezier te doen.

Uiteraard maakt dit soort van e-mail de minst gevaarlijke « hoax » uit wat zijn inhoud betreft. Door zijn aard, is de besmettingsgraad ervan echter zeer hoog. Blijf dus oplettend bij het uitkiezen van de humoristische berichten die u verstuurt alsook met de bestemmingen ervan. Dit gezegd zijnde, moet u niet nalaten om een goede grap met uw naasten te delen want humor is de beste bewaarder van lichaam en geest van man en vrouw...

Het gevaar dat een « hoax » voorstelt

Het is waar dat een hoax a priori geen bijzondere gevaren lijkt in te houden. Maar als men van wat dichterbij kijkt, stelt men vaak vast dat het aangewezen is ze te vermijden omdat ze de volgende gevaren kunnen inhouden :

- Ze bevatten valse beweringen die schade kunnen berokkenen aan het imago van een persoon of van een vennootschap en kunnen zelfs laster uitmaken ;
- Ze verspreiden geruchten die niet altijd even onschuldig zijn en die waarachtige informatie op het internet ongeloofwaardig maken : hoe kan men in die context nog een onderscheid maken tussen waar en onwaar ? Men moet zich dus altijd de vraag stellen of het gaat om informatie of om desinformatie ;
- Ze bezetten nutteloos de bandbreedte, vertragen de circulatie op de informaticanetwerken en kunnen, door een sneeuwbaaleffect, de mailservers verzadigen. Dit alles heeft een kost die, uiteindelijk, door de surfer wordt gedragen ;
- Ze bevatten valse alarmen (over virussen, dringende acties die moeten worden ondernomen, ...) en zorgen voor een zekere onverschilligheid waardoor waarachtige berichten niet meer als geloofwaardig worden beschouwd ;
- Ze kunnen worden gewijzigd door hackers en kunnen dienen als drager van virussen die het fopbericht omvormen tot een werkelijke epidemie.

HOE HANDELEN ?

Zoals u wel zal hebben begrepen, kunnen veel fopberichten of « hoax » voor problemen zorgen en zelfs werkelijk gevaar inhouden. Wij raden u dan ook aan om :

- twee maal na te denken alvorens het bericht « domweg » en automatisch door te sturen naar uw gehele adressenbestand of een deel ervan ;
- te controleren of het bericht al dan niet een « hoax » is op de website www.hoaxbuster.com ;
- als het gaat om een beweerd virus, het bestaan van dit nieuw virus te controleren op gespecialiseerde websites, waaronder www.secuser.com.

Als, ten gevolge van of ondanks deze controles, u het bericht niettemin wenst te verzenden naar uw kennissen, **raden wij u ten zeerste aan om de e-mailadressen in te voeren in het « bcc » veld (Blind Carbon Copy) van uw e-mail** : zo ontvangt elke bestemming het bericht zonder dat de adressen van de andere bestemmingen zijn vermeld. Zo vermijdt men dat alle bestemmingen van de verzonden

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

e-mail de e-mailadressen van al uw kennissen kunnen zien en, aldus, beperkt men het risico op inzameling en gebruik ervan voor het verzenden van spam.

VOOR MEER INFORMATIE

De site bij uitstek inzake hoax : www.hoaxbuster.com ;

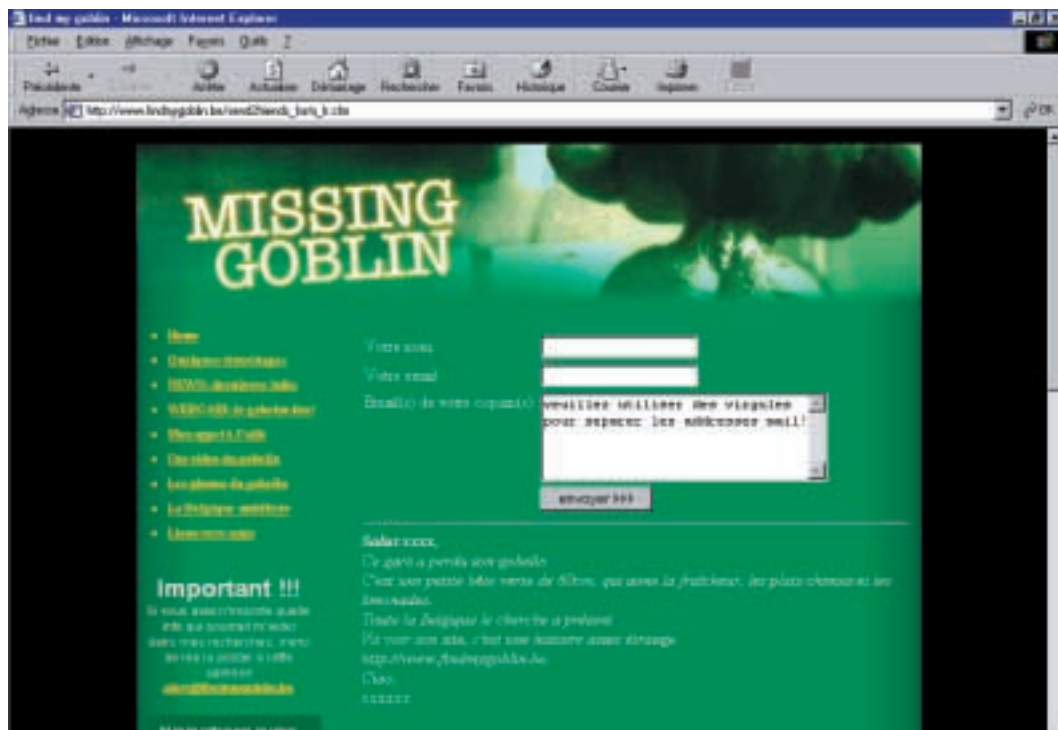
Talrijke voorbeelden worden eveneens gegeven op de website www.consumentenbedrog.be ;

Over virussen : www.secuser.com.

2. ÉLEKTRONISCHE BERICHTEN DIE U – TEGEN UW WIL – BETREK- KEN BIJ EEN PUBLICITEITSCAMPAGNE VOOR VIRALE MARKETING

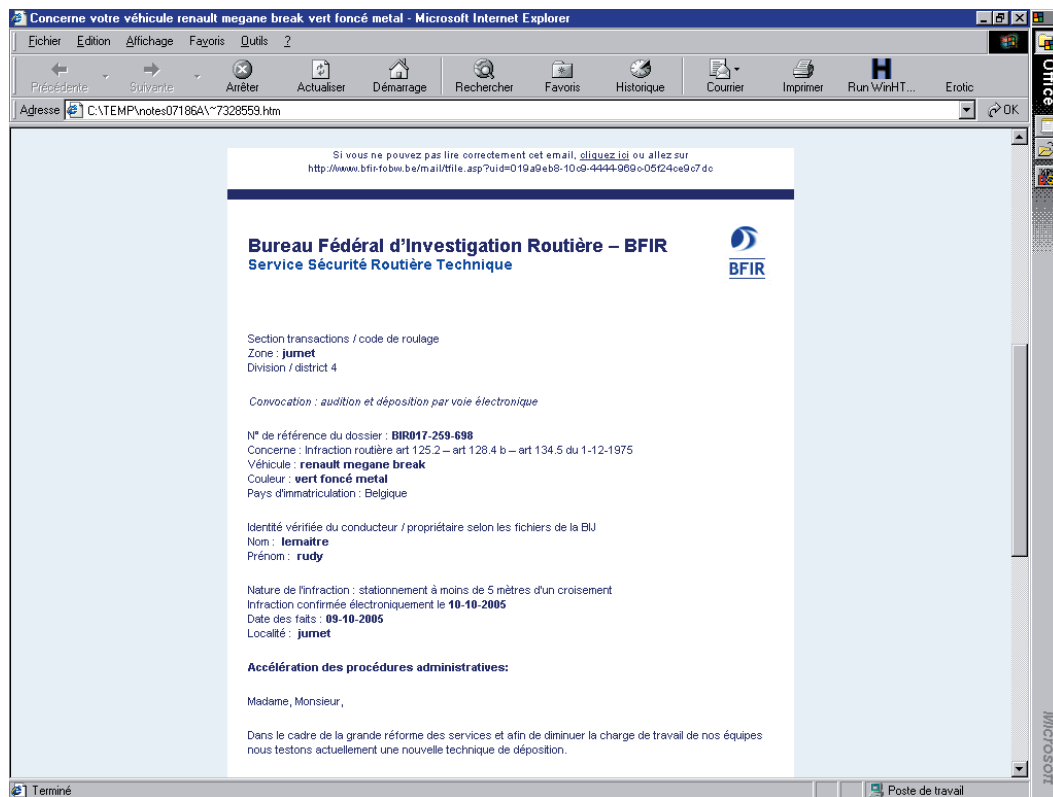
ILLUSTRATIES

Voorbeeld 1



« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Voorbeeld 2



Si vous ne pouvez pas lire correctement cet email, [cliquez ici](http://www.bfir.fobw.be/mail/Title.asp?uid=019a9eb8-10d9-4444-959c-05f24ce9c7dc) ou allez sur <http://www.bfir.fobw.be/mail/Title.asp?uid=019a9eb8-10d9-4444-959c-05f24ce9c7dc>

Bureau Fédéral d'Investigation Routière – BFIR
Service Sécurité Routière Technique

Section transactions / code de roulage
Zone : **jumet**
Division / district 4

Convocation : *audition et déposition par voie électronique*

N° de référence du dossier : **BIR017-259-698**
Concerné : Infraction routière art 125.2 – art 128.4 b – art 134.5 du 1-12-1975
Véhicule : **renault megane break**
Couleur : **vert foncé metal**
Pays d'immatriculation : Belgique

Identité vérifiée du conducteur / propriétaire selon les fichiers de la BJ
Nom : **lemaitre**
Prénom : **rudy**

Nature de l'infraction : stationnement à moins de 5 mètres d'un croisement
Infraction confirmée électroniquement le **10-10-2005**
Date des faits : **09-10-2005**
Localité : **jumet**

Accélération des procédures administratives:

Madame, Monsieur,

Dans le cadre de la grande réforme des services et afin de diminuer la charge de travail de nos équipes nous testons actuellement une nouvelle technique de déposition.



UITLEG

Regelmatig wordt men geconfronteerd met publiciteitscampagnes – zogenaamde “virale marketing” – die zowel op het internet als in de traditionele wereld worden gevoerd. Het is de stiekeme droom van alle marketingmensen : de consument-surfer die zelf promotor wordt.

Het concept is eenvoudig : het komt neer op het principe van de mond-tot-mondreclame, maar dan toegepast in een elektronische omgeving (eventueel gecombineerd met de traditionele omgeving), namelijk het verspreiden van een boodschap die tot verdere verspreiding ervan aanzet. De filosofie achter dergelijke virale marketing bestaat erin, dat er contacten worden gelegd met personen, niet zozeer via merkenstrategie, maar via een relatie, een vriend of een collega.

Virale marketing is van nature dynamisch : het bericht lokt een initiatief uit bij de ontvanger, zet hem ertoe aan iets aan te klikken, een antwoord te geven, de boodschap door te sturen, erover te praten...

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

Niet zelden nodigt de adverteerder de surfer bovendien uit om de boodschap nog verder te verspreiden en of stelt hem zelfs de middelen ter beschikking om de boodschap nog verder te verspreiden (bijvoorbeeld, een website met een formulier voor de inzameling van e-mailadressen dat voorziet in de automatische verzending van het bericht).

Om te zorgen voor een zo groot mogelijke verspreiding, kan dit soort van bericht verschillende aanpakken aannemen.

Deze aanpak kan humoristisch zijn, bijvoorbeeld door de verzending van grappige afbeeldingen of videoclips, door te verwijzen naar een grappige site, door een fopbericht te lanceren...

Deze aanpak kan eveneens ludiek zijn, bijvoorbeeld door de verspreiding van intrigerende informatie om een detectivespel te beginnen of van (soms extreem!) choquerende informatie (soms valse !) met als enig doel om de lezer wakker te schudden of te doen reageren, door on-line een spel te lanceren...

Het bericht kan er ook toe strekken om een dienst op te richten (elektronische kaarten, wallpapers, verdeling van stalen, kortingsbonnen, ...) of zelfs gebaseerd zijn op een systeem van peterschap.

In het eerste voormelde voorbeeld beperkt de campagne zich tot het verspreiden van valse opsporingsberichten (in de vorm van affiches en door een website en e-mails) van een schepsel dat gek is op limonade en tot het lanceren van een spel in de vorm van een intrige door de lezers uit te nodigen om berichten te laten waardoor men de plaatsen kan vermelden waar het zagezegd vermiste schepsel zagezegd zou zijn opgemerkt.

Zoals het beeld van dit voorbeeld aantoont, biedt de website die gewijd is aan deze campagne te dien einde een formulier aan waar de surfers hun e-mailadres van hun kennissen kunnen inschrijven, zodat het opsporingsbericht in kwestie ook naar hen kan worden gestuurd.

Er wordt geen enkele vermelding of informatie gegeven aan de hand waarvan men zou kunnen vaststellen dat men zich bevindt in het kader van een publiciteitscampagne. Het is slechts op het einde van de publiciteitscampagne (4 tot 6 weken later) dat het product wordt ontsluit dankzij de informatie volgens dewelke het schepsel is teruggevonden en waarbij deze laatste het product van een bekend merk in de hand houdt...

In het tweede hoger vermelde voorbeeld ontvangt u een e-mail (het gaat hier om een beeld van uw browser, dat een kopie uitmaakt van de ontvangen e-mail) waarin

u wordt gemeld dat u een verkeersinbreuk hebt begaan en waarin u wordt uitgenodigd om telefonisch (door op een ad hoc knop te drukken die in de e-mail wordt geplaatst) contact op te nemen met een lid van de openbare macht.

Hetgeen intrigerend is voor u en u doet denken dat het niet gaat om een fopbericht of om een reclamebericht in het kader van een campagne van virale marketing, is dat het bericht authentiek lijkt en vooral dat de informatie die in het bericht wordt gegeven (naam, voornaam, merk en kleur van de wagen) wel degelijk de uwe is !

U wordt er dus toe aangezet om te klikken op de oproepknop in kwestie. Op dat ogenblik, hoort u de beltoon van uw GSM en bent u in contact met de beweerde politiemans die de inbreuk heeft vastgesteld. In werkelijkheid, gaat het om een telefonisch fopbericht. Een bericht verwittigt u dat u werd gefopt door een vriend. Om zijn identiteit te weten te komen, volstaat het een bepaalde website te raadplegen, die reclame maakt voor een nieuw model van wagen...

Fopberichten doen u weliswaar lachen, maar houden een risico in op verwarring of misverstanden, om nog maar te zwijgen over het feit dat de surfer in de toekomst wel eens geen rekening zou kunnen houden met een – ditmaal ernstig – bericht afkomstig van gerechtelijke of administratieve autoriteiten, denkende dat het opnieuw om een fopbericht gaat !

Het voornaamste doel van de adverteerder bestaat er, in de campagnes van virale marketing, uiteindelijk altijd in om de verkoop van een product of een dienst te bevorderen, zelfs indien, in de praktijk, het publicitair karakter van het bericht of van het merk niet altijd vanaf het begin van de campagne blijkt.

Publiciteitscampagnes die steunen op de techniek van virale marketing zijn doorgaans zeer efficiënt. Het bijvoeglijk naamwoord « viraal » is in dit opzicht illustratief : het beschrijft het fenomeen van verspreiding dat, onder meer op het internet, wordt gekenmerkt door een systeem van piramidale verspreiding en een snelheid van overdracht die uiteraard doet denken aan de wijze van overdracht van een virus, van een epidemie.

HOE HANDELEN ?

Zelfs indien ze niet altijd getuigen van goede smaak, houden de publiciteitscampagnes van virale marketing zeker geen gevaar in dat vergelijkbaar is met dat van

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

de Nigeriaanse brieven, valse loterijen of andere gelijkaardige gevallen van oplichting. Deze campagnes zijn trouwens op zich niet wettelijk verboden.

Desalniettemin, heeft de Algemene Directie Regulering en Organisatie van de Markt van de FOD Economie, KMO, Middenstand en Energie de adverteerders en publiciteitsagentschappen eraan moeten herinneren dat dit soort van campagne eveneens overeenkomstig de wettelijke bepalingen moet worden gevoerd, o.m. overeenkomstig de wet van 14 juli 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument en de wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij.

U vindt een gedetailleerde voorstelling van de toepasselijke beginselen desbetreffend in onze nota « Hoe wettelijk is de virale marketing ? », dat op het volgende adres verkrijgbaar is :

http://economie.fgov.be/information_society/spamming/home_nl.htm.

Naast een herinnering aan de toepasselijke wettelijke beginselen, bestaat het doel van deze nota eruit om de consument-surfer bewust te maken van het spel waarin de adverteerder hem zal proberen te betrekken : het is niet verboden om aan een publiciteitscampagne van virale marketing deel te nemen, maar hij moet duidelijk weten dat hij aldus een deelnemer wordt in de verspreiding van een reclamebericht voor rekening van een merk.

Dat is de reden waarom de dienstverlener gehouden is om, als er een risico bestaat op verwarring in hoofde van de bestemming van het bericht, de vermelding « Reclame » aan te brengen op de dragers van deze campagne, zoals affiches, reclamebijlagen in de geschreven pers, de aan de campagne gewijde website, alsook eventuele e-mails die in dit kader worden verzonden en dit, vanaf het begin van de campagne van virale marketing.

Ook moet informatie worden verstrekt die het de consument mogelijk maakt om te bepalen wie zich verscholen houdt achter deze campagne (gegevens van de adverteerder en/of van het publiciteitsagentschap).

Uiteraard moet de consument zijn verantwoordelijkheden nemen en met kennis van zaken beslissen of hij al dan niet wenst deel te nemen aan het spel en of hij actief wil deelnemen aan deze campagne.

Het doel van deze nota bestaat er ook uit om de consument-surfer wakker te schudden voor de risico's die de inzameling en het gebruik van zijn persoonlijke gegevens, alsook van die van zijn kennissen, als hij deelneemt aan dergelijke campagne, kunnen voorstellen.

Ter herinnering, werkt de virale marketing volgens het beginsel van de mond-tot-mondreclame. Het idee is derhalve om de surfer ertoe aan te zetten om het bericht naar zijn gehele adressenbestand te versturen. **In dit kader, geven wij u twee essentiële tips.**

De eerste tip is de volgende : om te vermijden dat alle bestemmingen van de doorgestuurde e-mail de e-mailadressen van kennissen kunnen zien en, aldus, het risico op inzameling en gebruik ervan voor spamming te beperken, **raden wij de afzender ten strengste aan om de e-mailadressen in te voeren in het « bcc » veld (Blind Carbon Copy) van zijn e-mail.** Zo ontvangt elke bestemming het bericht zonder dat de adressen van de andere bestemmingen zijn vermeld.

64

De tweede tip is de volgende : als een website u vraagt om het e-mailadres van één of meerdere van uw kennissen in te voeren in een formulier met het oog op de mededeling van dergelijke acties, informatie, promoties, enz., hou er dan rekening mee dat u dat niet alleen zonder medeweten van uw kennis doet, maar dat u bovendien niet zeker bent dat de websiteverantwoordelijke het medegedeelde adres niet voor andere doeleinden zal gebruiken. (niet-vermelde promotie-acties, verkoop van adressen aan derden, enz.). **Zodoende draagt u in zekere mate bij tot de verhoging van het aantal spamberichten die uw kennissen riskeren te ontvangen ! Is dat wat ze van u verwachten ? Het is aan u om uw verantwoordelijkheden te nemen... Als u uw kennissen op de hoogte wil brengen van interessante initiatieven, stuur hen dan liever rechtstreeks een e-mail, dan hun adres in te schrijven op een formulier op een website waarvan u niets weet. Dat is zoveel gemakkelijker !**

De lezer vindt de volledige informatie over deze problematiek in voormelde nota van de FOD Economie.

VOOR MEER INFORMATIE

Nota van de FOD Economie inzake de wettelijkheid van virale marketing :
www.economie.fgov.be/information_society/spamming/home_nl.htm .

« De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. »

De website « hoaxbuster » : www.hoaxbuster.com ;

De website « Consumentenbedrog » van het OIVO : www.consumentenbedrog.be.

November 2006

Algemene Directie Regulering en Organisatie van de Markt

Cel elektronische economie

