Comment faire une plainte auprès d'un FAI et/ou de la police ?

N'est-ce pas agaçant et frustrant de recevoir et de voir presque chaque jour des courriers électroniques (courriels, mails) illégaux dont nous ne pouvons nous défendre ? En dehors de l'effet que nous les recevons sans les avoir sollicité, ces courriers encombrent le trafic sur Internet. De ce fait les **FAI**[1] doivent augmenter la capacité de leurs serveurs ce qui est un apport supplémentaire de frais, frais que tôt ou tard nous serons facturés d'une manière ou d'une autre pour notre abonnement !

Il existe bien des logiciels „**antispam**" gratuits et payants, mais ils ne résolvent pas le problème, car ils ne font rien d'autre que de bloquer les adresses non désirées et/ou le contenu non sollicité. Pourtant les expéditeurs de ces courriers continuent bel et bien **leur sale besogne**. **Et c'est là, à la racine du problème qu'il faut commencer, essayer d'éliminer d'une manière légale les polluposteurs**[2] **(expéditeurs de spam).**

Éliminer légalement les polluposteurs ?

Les expéditeurs de spam, de courrier phishing et d'autres arnaques peuvent être repérés par le protocole d'envoi du courrier électronique. Certes, il y a des techniques de camouflage pour cacher une **adresse IP** [3]d'un ordinateur connecté à Internet, mais la plupart de ces expéditeurs sont des internautes voulant se procurer un peu d'argent de poche, sachant qu'avec ces méthodes de spamming les chances y sont grandes d'y arriver.

Mais soit qu'ils ne connaissent pas l'illégalité de ces actions et/ou ils s'en foutent carrément, sachant aussi qu'il est très difficile de faire le traçage de l'origine de leurs courriers électroniques non sollicités et aussi que les autres internautes ne connaissent pas (encore) les techniques de retraçage ! Pour les professionnels de ces expéditeurs de courrier non sollicité, vous ne saurez rien faire, mais ils seront repérés tôt ou tard par les professionnels d'antifraude des services de la police judiciaire et d'autres organismes…

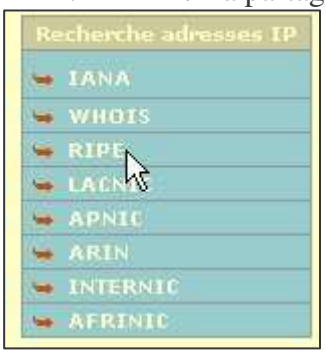
Les amateurs du spamming, du phishing et d'autres arnaques ne connaissent pas leur visibilité sur internet et de cette façon il nous est facile pour les repérer, de dévoiler leur **FAI** et de faire ensuite une plainte auprès de leur **FAI** et/ou de la police !

Quelques explications auparavant pour mieux comprendre :

1. Quand quelqu'un souscrit auprès d'un **FAI** pour recevoir un compte Email, il doit accepter les **T.O.S.** (**Termes Of Service**), les conditions générales d'utilisation de son compte. Dans ces **TOS** il est bien stipulé que nul a le droit d'offenser, ni d'envoyer du spam etc. Ce contrat, s'en est un, mais digital, vous l'acceptez en cochant la case que vous êtes d'accord avec ces termes d'utilisation. **C'est comparable à signer un contrat sur papier !**
2. Chaque ordinateur qui se connecte à Internet reçoit une **adresse IP, statique et/ou dynamique.** Cette **adresse IP** est comparable avec la plaque généalogique de votre voiture. Avec cette **adresse IP** il est possible de déterminer le **FAI** et le pays d'origine, mais pas la personne expéditrice.
3. **Les adresses IP sont gérées et distribués par l'IANA**. http://www.iana.org

[1] **F.A.I. : Fournisseur d'Accès Internet.**
[2] **Polluposteur : Expéditeur de spam (courrier non sollicité).**
[3] **Adresse IP** : **Adresse d'identification de l'ordinateur lors connexion à Internet, comparable à la plaque généalogique de la voiture.**

4. **L'IANA** a partagé cette distribution **d'adresses IP** en différentes parties du globe :



APNIC : Asia Pacific Network Information Centre
ARIN : American Registry for Internet Numbers
ACNIC : Latin American and Caribbean Internet Addresses Registry
RIPE : Réseaux IP Européens
AFRINIC : African Network Information Center
IANA : Internet Assigned Numbers Authority

Sachant maintenant que **toute personne connectée à Internet dispose d'une adresse IP** et quand elle se balade sur Internet, **cette adresse IP est toujours visible par tout le monde**. Comparable quand vous voyagez dans le monde, vous êtes visibles, les autres gens vous voient, sans connaître votre identité !

La même chose quand vous envoyez un courrier électronique à d'autres personnes, dans les propriétés de ce courrier votre **adresse IP** sera visible, ce qui est tout à fait normal. Quand vous envoyez une lettre à quelqu'un d'autre vous marquez aussi votre adresse expéditrice.

La pratique :

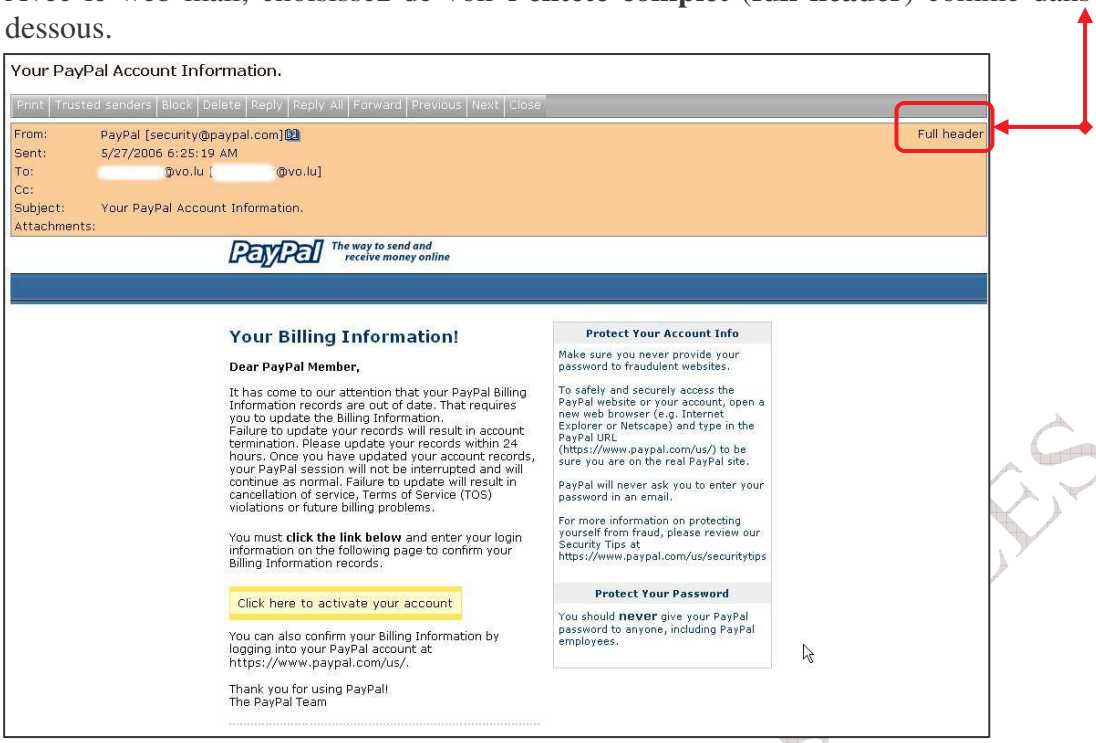
Pour déterminer qui est l'adresse expéditrice dans un courriel (email, courrier électronique), ouvrez le courrier électronique dans votre messagerie (programme email) et/ou sur le serveur de votre compte web mail.

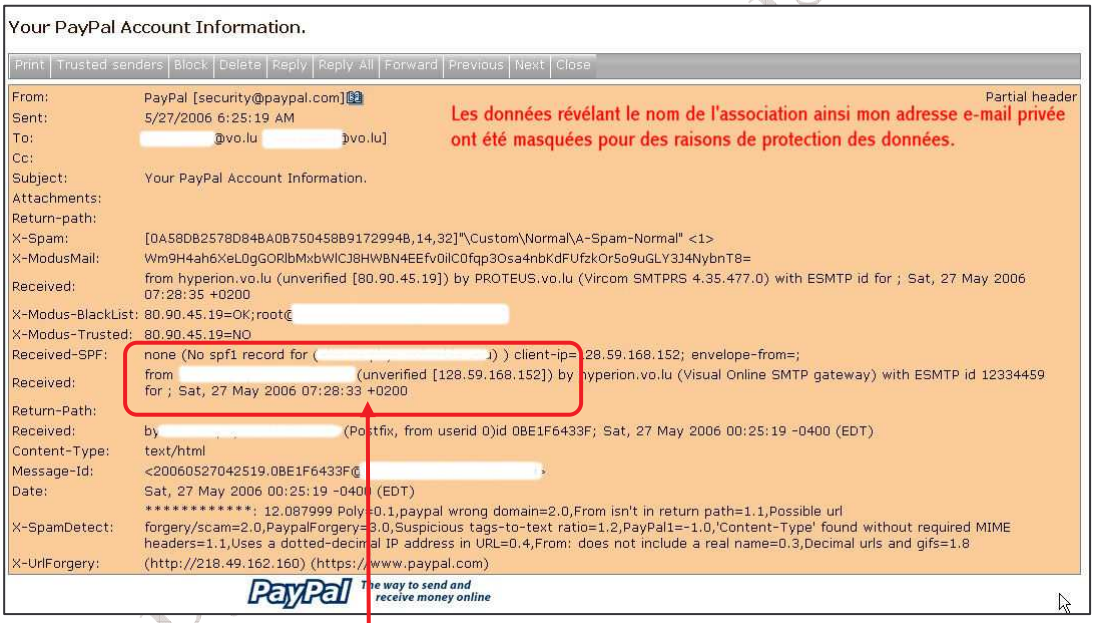
Messagerie électronique (programmes email, tels que Outlook, Incredimail, etc.) :

Ensuite en haut à gauche cliquer sur „**fichier**“, suivi de „**propriétés**“. Maintenant choisissez „**Entête ou Contenu**“. Vous verrez à ce moment (à première vue) un tas de chiffres incompréhensibles.

Web mail :

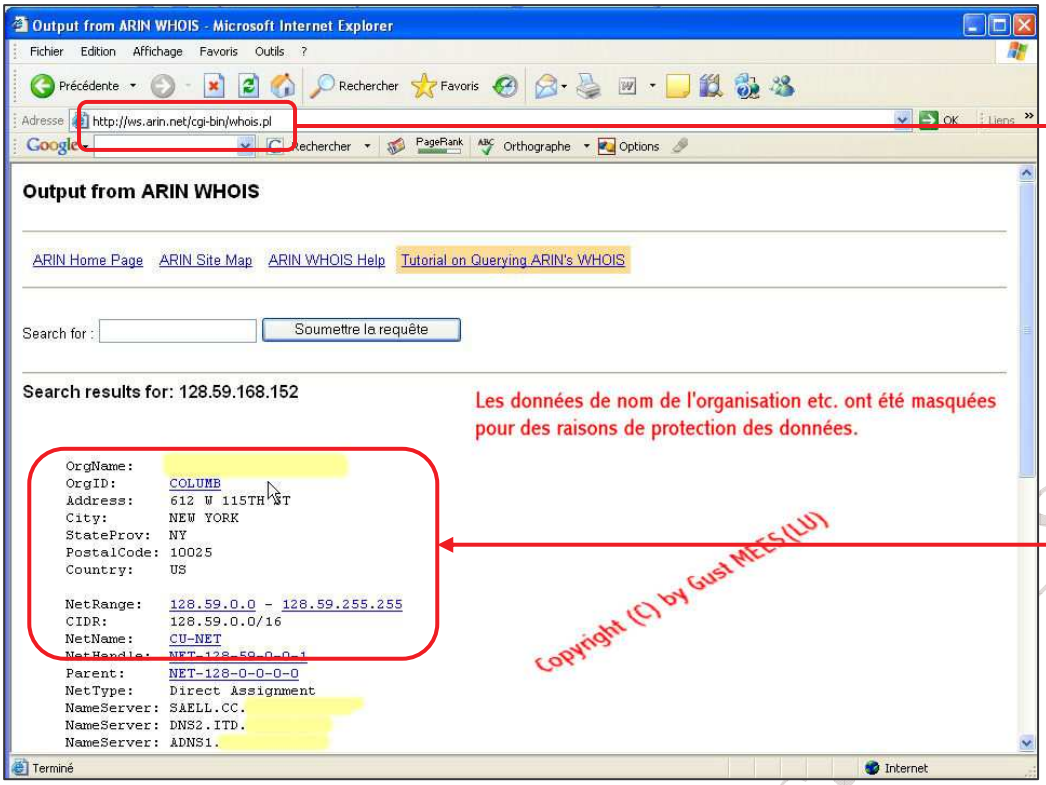
Avec le web mail, choisissez de voir **l'entête complet** (**full header**) comme dans notre exemple ci-dessous.



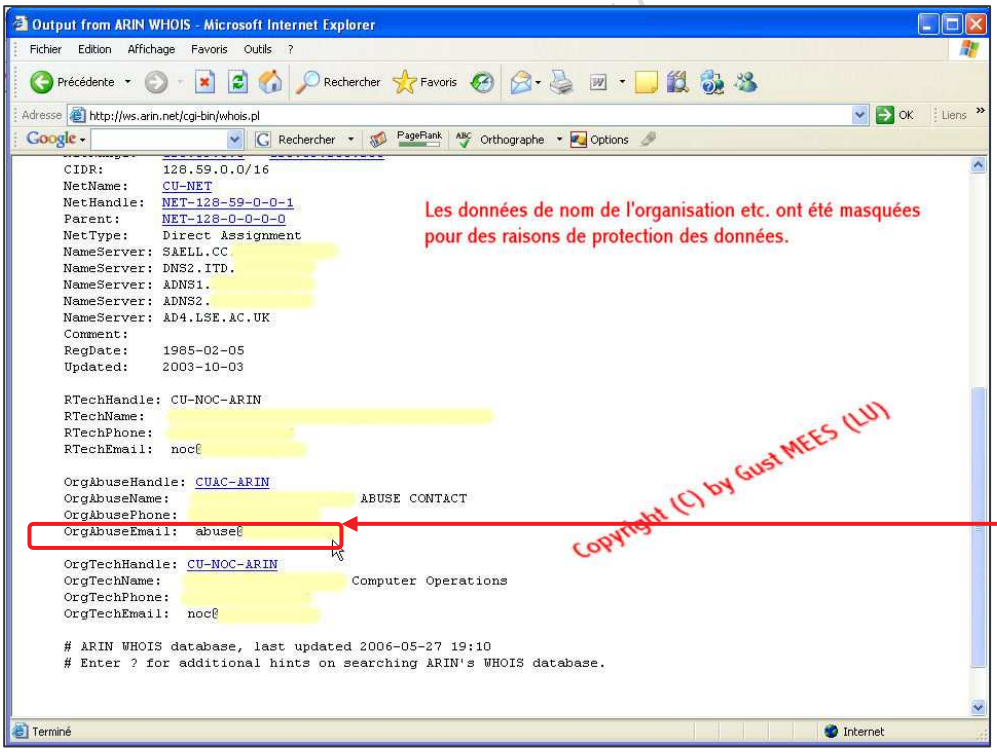


L'adresse IP expéditrice est bien marquée ici et nous pouvons l'utiliser pour faire la recherche du **FAI**.

Pour rechercher l'adresse IP souvenez-vous de ce qui a été discuté ci-dessus.



Ici le service de l'**ARIN a été utilisé qui indique clairement le propriétaire du nom de domaine (adresse IP convertie).**



En naviguant un peu plus vers le bas de cette page, vous verrez une **adresse de courrier où vous pouvez adresser la plainte officielle : abuse@...**

Ayant l'adresse du courrier électronique où il nous est possible d'adresser la plainte, dans notre exemple il s'agit d'une attaque de „**phishing**[4]**"**, nous pouvons préparer notre courrier électronique, qui doit contenir obligatoirement les éléments suivants (pour notre exemple) :

- Le sujet : **ABUSE /** type de l'attaque, dans notre exemple „**Phishing attack"**.
- La description exacte de votre plainte au début du courrier électronique.
- L'entête complète du courrier reçu.
- De préférence une copie de vos recherches sur l'adresse IP.
- Une phrase mentionnant que vous avez envoyé une copie aux services de la police locale.
- Une phrase de remerciement pour la coopération.

Il est préférable d'écrire le texte du courrier électronique en anglais. Pour ceux qui ne sont tellement familier avec la langue de Shakespeare, voici ci-dessous un texte type pour copier :

Texte type:

Hello

Some of your customers are trying again to send out "Phishing attacks"(à remplacer par votre texte) of the "PAYPAL TYPE". Please remember them your **T.O.S.** (Terms of service) and also **to STOP immediately**. Please consider this mail as an official complaint. A copy of this mail is also sent to the Luxembourgish police!
Please find below the full e-mail header as well as the "**whois query**".
Many thanks in advance for your cooperation.
Kind regards:
Votre nom

Par copier-coller (copy&paste) positionnez ici l'entête complet (full header) du courrier électronique.

[4] **Phishing = usurpation d'identité**

Exemple pratique de la plainte mentionnée ci-dessus :

Hello

Some of your customers are trying again to send out "**Phishing attacks**" of the "**PAYPAL TYPE**". Please remember them your **T.O.S. (Terms of service)** and also to STOP immediately. Please consider this mail as an official complaint. **A copy of this mail is also sent to the Luxembourgish police!**
Please find below the full e-mail header as well as the whois query.
Many thanks in advance for your cooperation.

Kind regards:

Gust MEES
Formateur pédagogique TIC
Partenaire officiel du Ministère de l'Économie, projet **CASES** http://www.cases.lu
Partenaire officiel du Ministère de l'Éducation, projet **MySecureIT** http://www.mysecureit.lu
Membre de l'**Internet Society of Luxembourg** http://www.isoc.lu
Editor of the online security magazine "**Internet Monitor**" http://www.internetmonitor.lu

---

FULL HEADER

From: PayPal [security@paypal.com] Partial header
Sent: 5/27/2006 6:25:19 AM
To: **my email address**
Cc:
Subject: **Your PayPal Account Information.**
Attachments:

Return-path:
X-Spam: [0A58DB2578D84BA0B750458B9172994B,14,32]"\Custom\Normal\A-Spam-Normal" <1>
X-ModusMail:
Wm9H4ah6XeL0gGORlbMxbWlCJ8HWBN4EEfv0ilC0fqp3Osa4nbKdFUfzkOr5o9uGLY3J4NybnT8=
Received: from hyperion.vo.lu (unverified [80.90.45.19]) by PROTEUS.vo.lu (Vircom SMTPRS 4.35.477.0) with ESMTP id for ; Sat, 27 May 2006 07:28:35 +0200
X-Modus-BlackList: 80.90.45.19=OK;**root@nom…=OK**
X-Modus-Trusted: 80.90.45.19=NO
Received-SPF: none (No spf1 record for (**nom…….)**) client-ip=**128.59.168.152**; envelope-from=;
Received: from nom… (unverified [**128.59.168.152**]) by hyperion.vo.lu (Visual Online SMTP gateway) with ESMTP id 12334459 for; Sat, 27 May 2006 07:28:33 +0200
Return-Path:
Received: **by nom…** (Postfix, from userid 0) id 0BE1F6433F; Sat, 27 May 2006 00:25:19 -0400 (EDT)
Content-Type: text/html
Message-Id: **<20060527042519.0BE1F6433F@nom...>**

Date: Sat, 27 May 2006 00:25:19 -0400 (EDT)
X-SpamDetect: **********: 12.087999 Poly=0.1,paypal wrong domain=2.0,From isn't in return path=1.1,Possible url forgery/scam=2.0,PaypalForgery=3.0,Suspicious tags-to-text ratio=1.2,PayPal1=-1.0,'Content-Type' found without required MIME headers=1.1,Uses a dotted-decimal IP address in URL=0.4,From: does not include a real name=0.3,Decimal urls and gifs=1.8
X-UrlForgery: (**http://218.49.162.160**) (https://www.paypal.com)

Search results for: 128.59.168.152

OrgName: Nom…
OrgID: COLUMB
Address: 612 W 115TH ST
City: NEW YORK
StateProv: NY
PostalCode: 10025
Country: US

NetRange: **128.59.0.0 - 128.59.255.255**
CIDR: 128.59.0.0/16
NetName: CU-NET
NetHandle: NET-128-59-0-0-1
Parent: NET-128-0-0-0-0
NetType: Direct Assignment
NameServer: SAELL.CC.NOM…
NameServer: DNS2.ITD.NOM…
NameServer: ADNS1.NOM…
NameServer: ADNS2.NOM…
NameServer: AD4.LSE.AC.UK
Comment:
RegDate: 1985-02-05
Updated: 2003-10-03

Les données de nom de l'organisation, numéro téléphonique, adresse de courrier etc. ont été masqués afin de garantir la protection de vie privée.

RTechHandle: CU-NOC-ARIN
RTechName: **NOM… Computer Operations**
RTechPhone:
RTechEmail: noc@nom...

OrgAbuseHandle: CUAC-ARIN
OrgAbuseName: **"NOM…" ABUSE CONTACT**
OrgAbusePhone:
OrgAbuseEmail: **abuse@nom...**

OrgTechHandle: CU-NOC-ARIN
OrgTechName: **NOM… Computer Operations**
OrgTechPhone:
OrgTechEmail**: noc@nom...**

ARIN WHOIS database, last updated 2006-05-27 19:10
Enter ? for additional hints on searching ARIN's WHOIS database.

Récapitulatif :

Pour faire une plainte, il nous faut l'adresse IP de l'expéditeur qui se trouve dans l'entête du courrier électronique et qui est facilement identifiable quand il s'agit d'amateurs. Ayant localisé l'adresse IP il faut faire la recherche chez les **distributeurs d'adresses IP.**

Pour vous faciliter la tâche, la barre de navigation ci-contre est présente sur notre site Internet http://www.internetmonitor.lu sur le côté droit.

Connaissant ensuite le propriétaire du nom de domaine (adresse IP convertie), vous pouvez en extraire l'adresse email pour envoyer la plainte. Si c'est une firme sérieuse, cette adresse commence par **„abuse@.....“**.

Maintenant il suffit de préparer le courrier électronique. Pour ceci il faut intégrer l'adresse email trouvée et inclure aussi le sujet **„ABUSE :.....“**, suivi de l'adresse email de la police locale dans le champ „**Cc**“.
Pour le Luxembourg cette adresse est „info@police.public.lu“.

Ensuite copiez le texte en anglais „**Texte type**“ dans la partie texte de votre courrier électronique, suivi de l'entête du courrier reçu, ainsi que le résultat trouvé de votre recherche d'adresse IP.

Votre courrier électronique pour faire une plainte est prête à envoyer. Vérifiez en comparant avec l'exemple pratique mentionné ci-dessus.

De cette façon, si tout le monde faisait pareil, au moins les amateurs seraient éliminés. Quand les FAI (ISP) reçoivent cette plainte et qu'ils la prennent au sérieux, la personne qui vous a adressé ce courrier perdra son compte Internet et elle sera marquée dans une liste noire. Cette liste noire est consultable par tout FAI. Si cette personne essaie de trouver un autre FAI, elle sera avertie d'avance de ne plus faire d'abus. En plus s'il y a suite par la police cette personne risque de graves ennuis !

En ce qui concerne les FAI, chaque abonné (vous aussi) doit accepter les conditions générales d'utilisation, les TOS en anglais (Termes Of Service), AGB (Allgemeine Geschäfts Bedingungen) en allemand.
Veuillez trouver ci-dessous un extrait des termes de service (TOS) d'un FAI luxembourgeois. Pour les FAI d'autres pays les TOS sont similaire.

Extrait TOS

P&T Luxembourg :

http://www.ept.lu/upload/FRWDES67ED34/CE7CB9AFF47B/downloads/10938F1916C10.pdf

Extrait :

LES LIGNES DIRECTRICES POUR L'UTILISATION DE L'INTERNET DES P&T: VOTRE SÉCURITÉ NOUS IMPORTE!

Pour que vous puissiez travailler en toute tranquillité sur Internet, P&T Luxembourg a élaboré certaines règles pour l'utilisation de l'Internet. Ces règles vous garantissent que votre expérience Internet se passe dans les meilleures conditions possibles. Qui n'a pas déjà entendu parler de « spamming », « spoofing » ou « hacking » ? C'est pourquoi nous avons élaboré nos lignes directrices pour l'utilisation de l'Internet: pour nous donner les moyens de lutter efficacement contre tout abus d'Internet.

LIGNES DIRECTRICES POUR L'UTILISATION DE L'INTERNET

Abuser du système est strictement interdit. En cas d'abus, P&T Luxembourg se réserve le droit de résilier ou de modifier immédiatement l'accès au service Internet et de facturer les frais engendrés par l'abus du système par le client. Ci-après se trouve une liste d'actions définies comme abus du système. Cette liste n'est pas exhaustive, toute action pour laquelle un doute existe doit être soumise à P&T Luxembourg pour évaluation (tél.: 12422 (gratuit); fax: 12423 (gratuit); e-mail: internet@ept.lu).

Les actions qui constituent un abus du système comprennent, mais ne se limitent pas à:

1. toute tentative de contourner les mesures d'authentification des usagers ou de sécurité de tout hôte (ordinateur qui exécute des applications), réseau ou abonnement de P&T Luxembourg ou d'Internet en général ("cracking");

2. toute tentative, quelle qu'en soit la nature, pour interférer avec ou de refuser le service à tout utilisateur ou hôte sur Internet;

3. la contrefaçon de courrier électronique ou de messages USENET, de quelque manière que ce soit;

4. l'envoi de quantités volumineuses de courriers électroniques non sollicités ("junk mail", "spamming"); ceci comprend l'inclusion ou la tentative d'inclusion d'adresses de courrier électronique à toute liste d'envoi pour courrier électronique sans l'accord préalable et explicite du destinataire;

5. transférer ou envoyer des "chaînes de lettres" (transferts multiples) de quelque nature que ce soit;

6. l'envoi de messages non appropriés aux groupes de nouvelles USENET, p.ex. l'envoi sans discrimination d'un nombre élevé de messages non sollicités ("spamming") à des groupes de nouvelles ou l'envoi de fichiers binaires encodés à des groupes de nouvelles USENET dont le nom n'indique pas clairement qu'ils existent à cette fin;

7. la tentation d'annuler, de remplacer ou d'interférer autrement avec du courrier électronique ou des messages USENET autres que ceux qui sont originaires du client même;

8. le harcèlement, qu'il résulte du langage, de la fréquence ou de la taille du message;

9. l'utilisation d'un accès chez un autre ISP pour promouvoir un site web de P&T Luxembourg d'une manière non appropriée et/ou abusive;

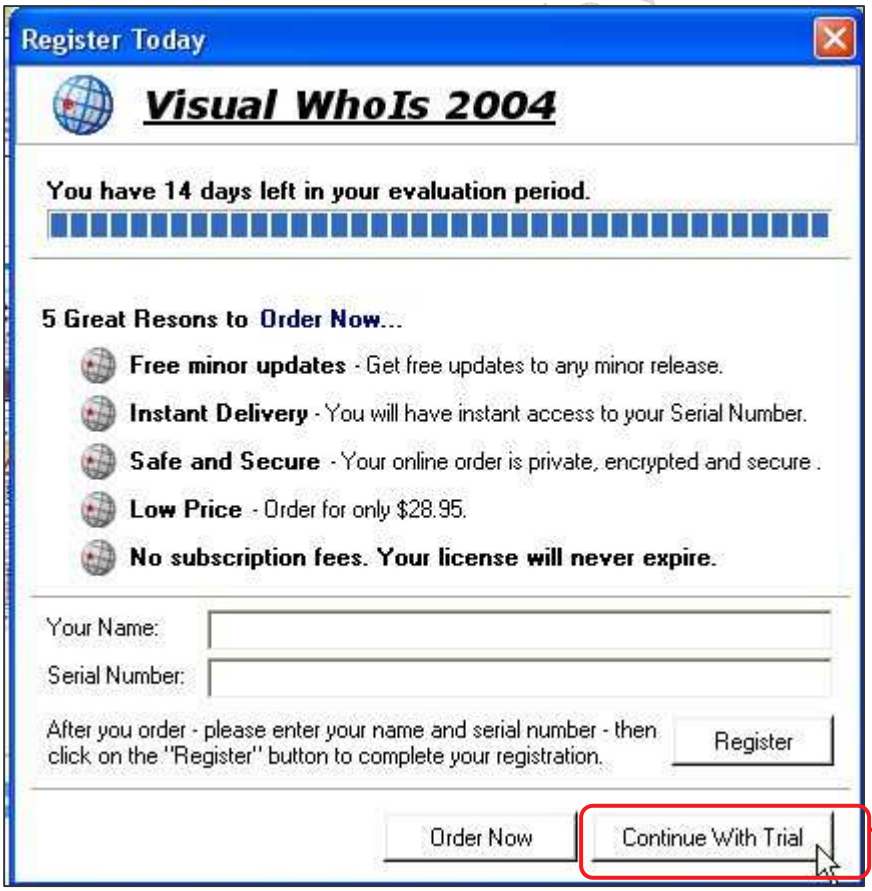
10. l'utilisation d'un accès ou d'une connexion réseau de P&T Luxembourg pour rassembler des réponses à des messages envoyés via un autre ISP qui ne respectent pas les présentes règles ou celles de l'autre ISP;

Outils de recherche automatique de l'adresse IP

Afin de vous faciliter le travail, il est préférable de prendre recours à des logiciels qui vous simplifient la tâche de recherche pour identifier une adresse IP. Un logiciel très performant est „**Visual Whois".** Cet utilitaire est capable de vous afficher le propriétaire de chaque site Internet visité, de faire un traçage d'adresses IP, de contrôler des adresses e-mail, ainsi que de tracer la route complète qu'un courrier électronique a pris. Le logiciel peut être téléchargé à l'adresse suivante :

http://www.softwareriver.com/

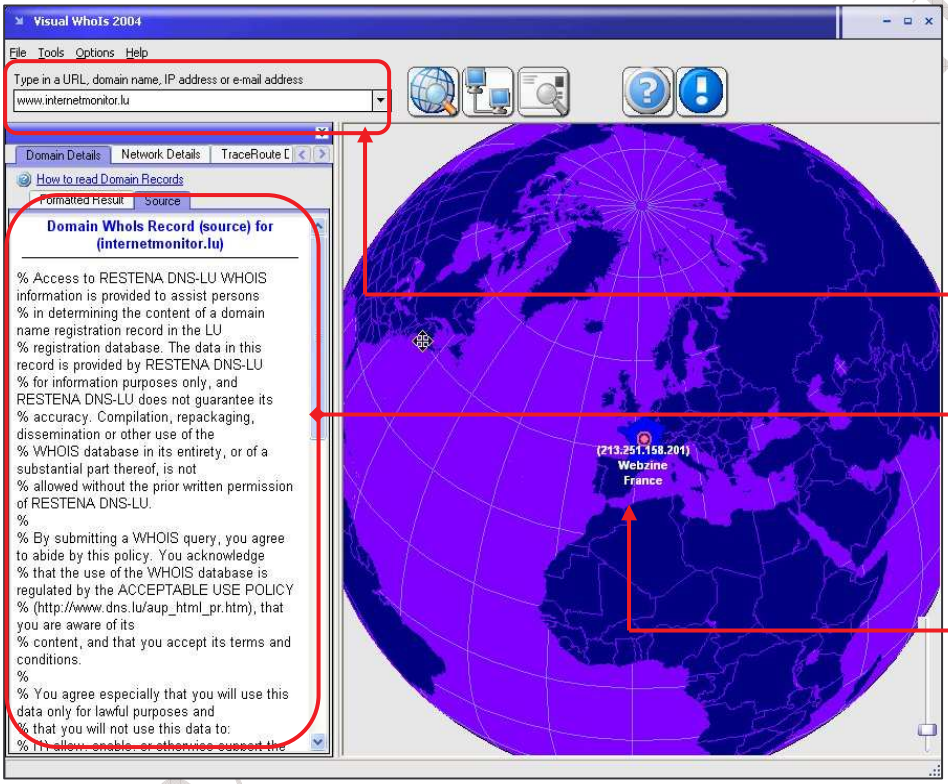
Après son installation l'utilitaire s'intègre automatiquement dans l'onglet „**Outils",** dont il suffit de cliquer sur „**Locate Using Visual Whois 2004"**.



La fenêtre ci-contre s'affiche, indiquant que le logiciel est disponible en **version d'évaluation de 14 jours,** ainsi qu'en **version payante de $28.95.**

Si vous choisissiez d'utiliser la version d'évaluation, cliquer sur le bouton „**Continue With Trial"**.

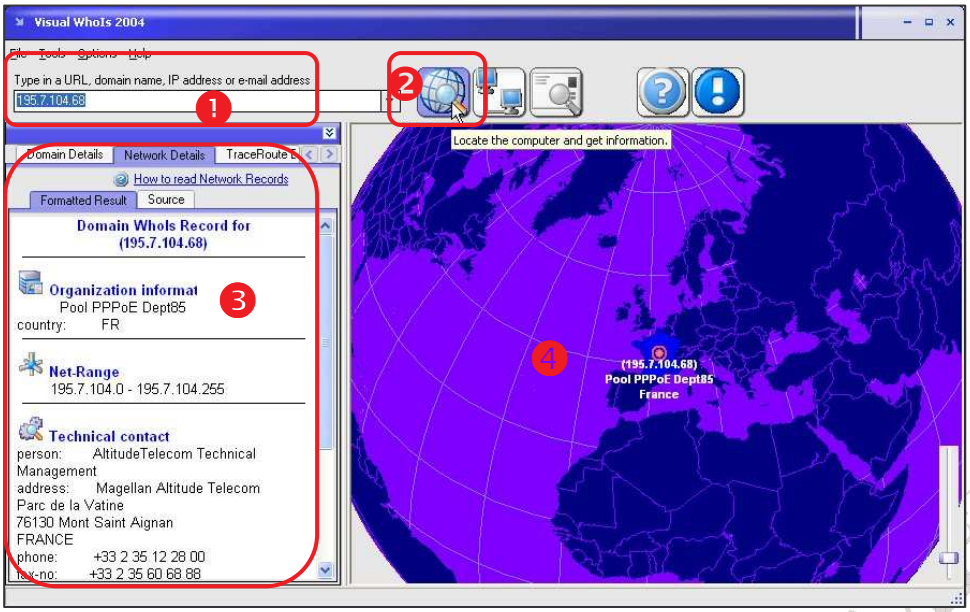
Le firewall (pare-feu) vous alerte alors (sil est bien configuré) que l'utilitaire veut se connecter à Internet. Confirmez en cliquant sur le bouton „**OK**“.



L'interface du logiciel s'affiche, comme montré ci-contre. Le site Internet que vous aviez visité récemment (votre page de démarrage) est automatiquement intégré dans le **champ de requête**.
Dans le champ de texte, marqué par l'onglet „**Source**“ seront affichées les données du **propriétaire du nom de domaine.**

Dans le champ graphique vous trouverez le **lieu de l'hébergeur (host)**.

Utiliser le logiciel „Visual Whois“ pour tracer les adresses IP :



Tapez **l’adresse IP** que vous aviez trouvé dans l’entête du courrier électronique **dans le champ de requête** 1 et cliquer ensuite sur le bouton **„Locate the computer and get information“** 2.
Votre requête est maintenant traitée et le résultat est affiché dans le champ de texte, marqué par l’onglet **„Formatted Result“** 3. En plus du résultat obtenu, l’interface graphique 4 montre la **localisation géographique de l’hébergeur**.

Il ne reste plus qu’à extraire l’adresse de courrier électronique qui sert pour déclarer l’abus à l’ISP en question.

Plus de plaintes que les ISP et/ou la police recevront, plus qu’ils surveilleront. Si le client ne bouge pas, rien ne se passera. Si la masse des clients se plaint, le fournisseur doit réagir.