

Groupe de travail sur le pourriel

Document d'accompagnement des
Pratiques exemplaires recommandées
pour les fournisseurs de service Internet
et autres exploitants de réseaux

par John Levine

mai 2005

Sommaire

Le courriel demeure l'application Internet la plus utile depuis 20 ans, malgré la prolifération des pourriels et autres usages abusifs. Toutefois, la grave menace que pose le pourriel a incité le gouvernement du Canada à créer un groupe de travail pour mettre en œuvre le *Plan d'action anti-pourriel pour le Canada*. Comme les fournisseurs de service Internet (FSI) et autres exploitants de réseaux peuvent empêcher plusieurs types d'usage abusif du courriel et en détecter d'autres, on a mis sur pied un sous-groupe de travail consacré à la gestion des technologies et des réseaux, qui a élaboré une série de pratiques exemplaires d'ordre technique afin de responsabiliser davantage les expéditeurs de courriel tout en perturbant le moins possible les activités des utilisateurs.

Étant donné la nature technique du document sur les pratiques exemplaires, le présent document d'accompagnement a été élaboré pour expliquer les concepts en jeu et montrer la façon dont ces pratiques aideront à s'attaquer au problème du pourriel.

Tour d'horizon du courriel Internet

À l'époque où le courriel Internet a vu le jour, les réseaux et les ordinateurs étaient beaucoup plus lents et moins fiables qu'aujourd'hui, et Internet et son prédécesseur ArpaNet ne faisaient pas l'objet d'usages abusifs. C'est pourquoi la norme utilisée pour transmettre le courriel, connue sous le nom de « Simple Mail Transfer Protocol » (SMTP), est très efficace pour acheminer les messages, mais elle l'est beaucoup moins pour ce qui est de retracer et de responsabiliser l'expéditeur. Le protocole SMTP prend la forme d'un système de stockage et de transfert, si bien que l'ordinateur de l'expéditeur peut envoyer un courriel directement à celui du destinataire. Toutefois, les messages passent le plus souvent d'un ordinateur à l'autre en plusieurs étapes — par exemple, de l'ordinateur de l'expéditeur au serveur de courriel sortant de son FSI, puis au serveur de courriel entrant du FSI du destinataire et à son serveur de courriel interne et, enfin, à l'ordinateur du destinataire.

En jargon Internet, un ordinateur qui gère l'accès à Internet est appelé « hôte ». Dans toute transaction entre deux ordinateurs, l'un est considéré comme le « serveur » et l'autre comme le « client ». Dans le cas du courriel SMTP, l'ordinateur qui envoie le message est le client, et celui qui le reçoit est le serveur. Un serveur de courriel est donc un hôte qui reçoit des messages destinés à ses utilisateurs. Il est possible que l'hôte remplisse différents rôles. Par exemple, un serveur de courriel qui a reçu un message pourra faire office de client pour l'envoyer à un autre serveur.

Chaque ordinateur hôte a une adresse IP (Internet Protocol), c'est-à-dire un numéro similaire à un numéro de téléphone, que les autres hôtes utilisent pour y accéder. Comme il est plus facile de se rappeler un nom qu'un numéro, on donne aussi un nom aux systèmes hôtes et aux systèmes de courriel (par exemple, **exemple.ca** et **ic.gc.ca**). Le système de noms de domaine d'Internet sait quel nom correspond à quelle adresse IP. On utilise aussi des noms de domaine dans les adresses de courriel : **pm.gc.ca** est le domaine dans l'adresse de courriel **pm@pm.gc.ca**.

Pratiques exemplaires

1. Tous les registraires et hôtes canadiens de noms de domaine devraient publier des renseignements sur Sender Policy Framework (SPF) dans les fichiers de leur zone respective de serveur de nom de domaine le plus tôt possible.

SPF est un système qui vise à détecter les messages contrefaits. Il permet au gestionnaire d'un domaine de courriel de publier la liste des adresses IP des hôtes autorisés à transmettre des courriels à partir d'adresses faisant partie de son domaine. Si tous les messages provenant d'un domaine sont envoyés à partir d'un point unique, comme c'est souvent le cas pour les utilisateurs qui envoient des messages en vrac et les petites entreprises, SPF peut aider à détecter la contrefaçon lorsqu'un courriel, dont l'en-tête indique qu'il provient de ce domaine, arrive d'une autre source.

Comme la plupart des courriels envoyés utilisent des noms de domaine contrefaits pour camoufler leur source, il est essentiel de pouvoir mettre en évidence la contrefaçon afin de retracer les courriels et de les empêcher d'entrer dans les réseaux.

2. Les FSI et autres exploitants de réseaux devraient limiter, par défaut, l'utilisation du port 25 par les utilisateurs finaux. Au besoin, la capacité d'envoyer ou de recevoir du courriel au moyen du port 25 devrait être limitée aux ordinateurs hôtes du réseau du fournisseur. L'utilisation du port 25 par les utilisateurs finaux devrait être permise au besoin ou être conforme à l'entente entre le fournisseur et l'utilisateur final et aux modalités de service.

Bien qu'il soit techniquement possible que les clients des FSI envoient des messages directement de leur propre ordinateur à celui du destinataire, l'utilisateur envoie généralement le message de son ordinateur au serveur de courriel de son FSI, qui l'envoie ensuite au destinataire. À l'origine, cette technique visait à accroître la fiabilité de la transmission, car le serveur de courriel du FSI peut essayer à nouveau d'envoyer les messages qui ne peuvent être livrés immédiatement. Nous ferons état d'autres avantages plus loin.

Pour éviter d'être détectés par le FSI de l'utilisateur, les polluposteurs et les auteurs de virus essaient souvent d'envoyer les messages directement de l'ordinateur des utilisateurs à celui des destinataires sans passer par le serveur de courriel du FSI. À l'origine, les polluposteurs ouvraient leur propre compte, mais ils utilisent maintenant les ordinateurs infectés des utilisateurs au moyen de vers ou de virus qui leur permettent de les contrôler à distance. Ces ordinateurs « contrôlés » sont appelés « zombies ».

Si le FSI limite l'accès des utilisateurs au port 25, soit le canal logique utilisé pour le courriel Internet, afin que l'utilisateur ne puisse qu'envoyer des courriels directement au serveur de courriel du FSI, le fournisseur sera au courant de tous les courriels envoyés par l'utilisateur d'un ordinateur et pourra prendre des mesures s'il détecte un comportement abusif.

Dans de rares cas, l'ordinateur de l'utilisateur a une raison légitime de contacter des serveurs de courriel autres que celui de son FSI (par exemple, lorsqu'un télétravailleur envoie des messages par le système de courriel de son employeur). C'est pourquoi le FSI doit être en mesure de permettre des exceptions au blocage du port 25, mais il s'agit d'une si faible proportion des utilisateurs que le fournisseur peut s'en occuper au cas par cas.

Les polluposteurs qui exploitent des réseaux de zombies abusent largement du port 25. En surveillant et en limitant l'utilisation de ce port, les FSI et autres exploitants de réseaux peuvent grandement freiner le pourriel. On a observé une nette diminution du volume de pourriels provenant des réseaux des FSI canadiens qui bloquent le port 25.

3. Les FSI et autres exploitants de réseaux devraient bloquer les pièces jointes aux courriels dont les extensions sont connues pour transporter des virus ou filtrer les pièces jointes en fonction des propriétés du contenu.

Un courriel Internet peut se composer d'un texte de message et de fichiers de données joints au message. Les pièces jointes sont extrêmement utiles (par exemple, pour envoyer des documents ou des fichiers de présentation à un collègue), mais ils sont largement utilisés par les auteurs de virus, qui créent des courriels et y joignent des copies du virus pour infecter l'ordinateur des destinataires qui ouvriront le message. Comme les types de fichiers joints utilisés par les auteurs de virus ne servent guère à des utilisations légitimes, les FSI peuvent et devraient les bloquer. (L'« extension » est la partie du nom d'un fichier qui suit le point et identifie le type de fichier.)

Le blocage des pièces jointes est utile tant pour les courriels entrants, afin d'empêcher les virus de s'immiscer dans le réseau, que pour les courriels sortants, afin de détecter les clients dont l'ordinateur est infecté par un virus.

Grâce à ces efforts, on réduira le risque qu'un pourriel renfermant un programme malveillant n'entre dans un réseau et ne dépose des virus et des vers pour créer et

exploiter des réseaux de zombies. En faisant échec aux réseaux de zombies, on pourra freiner le pourriel.

4. Les FSI et autres exploitants de réseaux devraient surveiller étroitement le volume de courriels entrants et sortants afin de repérer les activités inhabituelles dans le réseau et leur source, et prendre des mesures en conséquence.

Il est rare que le comportement d'un internaute utilisant le courriel change radicalement d'un jour à l'autre. Si l'utilisateur a envoyé 3 messages un jour et qu'il en envoie 10 000 le lendemain, il y a tout lieu de croire qu'un virus a commandé à son ordinateur d'envoyer des pourriels – il serait étonnant que cet utilisateur se soit fait autant de nouveaux amis en si peu de temps! De même, si un utilisateur qui reçoit généralement une dizaine de messages par jour commence à en recevoir 1 000, il y a vraisemblablement un problème.

Si un FSI constate une activité inhabituelle et qu'il réagit sans délai, il est souvent possible d'arrêter le pollupostage ou un autre usage abusif sur le fait, au lieu d'attendre que les victimes s'en rendent compte et se plaignent.

5. Les FSI et autres exploitants de réseaux devraient établir et maintenir de façon continue des processus efficaces et rapides pour la gestion et l'élimination des éléments de réseau infectés constituant une source de pourriel.

Les ordinateurs zombies, c'est-à-dire les ordinateurs personnels infectés par un vers ou un virus et contrôlés à distance par des pirates, constituent la principale source de pourriel. Comme ces ordinateurs continuent d'effectuer les fonctions habituelles, la plupart des utilisateurs ne savent pas que des pirates ont la haute main sur leur ordinateur.

Lorsqu'un FSI se rend compte que l'ordinateur d'un utilisateur fait l'objet d'un usage abusif, il doit d'abord suspendre l'accès de cet utilisateur au réseau pour mettre fin à cet usage, puis aider l'utilisateur à éliminer le ver ou le virus. Il s'agit d'une procédure complexe, qui nécessite à la fois des programmes antivirus et anti-logiciel espion, ainsi que des mises à jour obtenues auprès des fournisseurs de logiciels pour éviter la réinfection de l'appareil. Rares sont les utilisateurs qui peuvent enlever les vers de leur ordinateur sans aide. Le FSI est généralement la seule ressource à sa disposition qui possède les connaissances voulues pour l'aider.

Les FSI et autres exploitants de réseaux qui utilisent cette pratique exemplaire seront en mesure d'enrayer rapidement et efficacement les pourriels qui s'attaquent à leur réseau.

6. Les FSI et autres exploitants de réseaux devraient établir des processus interentreprises pertinents afin de réagir aux rapports d'incidents des autres exploitants de réseaux.

Les FSI et autres exploitants de réseaux se transmettent fréquemment les rapports faisant état des usages abusifs de leur réseau. Si un utilisateur envoie des pourriels, il est possible que son FSI l'apprenne grâce aux rapports d'autres fournisseurs dont les mécanismes de filtrage ont bloqué ses courriels.

Plus les FSI peuvent signaler un problème de façon rapide et efficace aux autres exploitants, plus le FSI qui approvisionne l'utilisateur en cause pourra régler le problème rapidement et, par conséquent, moins le volume de pourriels envoyés et reçus par différents réseaux sera élevé.

7. Les FSI et autres exploitants de réseaux ainsi que les fournisseurs de service de courrier électronique devraient communiquer leurs politiques et procédures en matière de sécurité à leurs abonnés.

Souvent, les utilisateurs ne peuvent constater d'emblée les effets des politiques des FSI en matière de sécurité. Par exemple, si un filtre de virus rejette un type de courriel en particulier, le destinataire s'en rendra compte uniquement si l'expéditeur remarque que le message ne s'est pas rendu à destination et qu'il l'en informe.

Chaque politique en matière de sécurité doit atteindre un équilibre : il faut empêcher les activités qui donnent souvent lieu à un usage abusif tout en permettant l'utilisation légitime de ces activités. Alors que la plupart des activités régies par les politiques en matière de sécurité ne donnent guère lieu à des utilisations légitimes, certaines politiques empêchent un volume modeste, mais appréciable d'utilisations légitimes. Si les FSI renseignent leurs utilisateurs sur leurs politiques, les internautes touchés pourront modifier leur façon de travailler et adopter des méthodes compatibles avec ces politiques. Par exemple, lorsqu'un FSI bloque le port 25, les utilisateurs qui doivent communiquer avec des serveurs de courriel sur d'autres réseaux peuvent généralement reconfigurer leur programme de courriel de manière à utiliser un port différent qui n'est pas sujet aux problèmes d'usage abusif observés dans le cas du port 25.

Le filtrage des pourriels constitue un sujet de préoccupation particulier, car les filtres mal configurés peuvent rejeter ou détruire un volume considérable de courriels voulus. Les FSI peuvent mettre à la disposition des utilisateurs une description des techniques de filtrage qu'ils utilisent, en précisant ce qui se produit lorsqu'un courriel est considéré comme un pourriel, et quelles sont les avenues à la disposition des utilisateurs qui estiment que des courriels légitimes ont été considérés comme des pourriels ou vice versa.

Les utilisateurs sont essentiels dans la lutte contre le pourriel. Si on les sensibilise au problème et aux mesures mises en place pour le régler, ils pourront mieux comprendre la situation et seront plus aptes à se protéger et, par le fait même, à protéger leur réseau hôte.

8. Les FSI et autres exploitants de réseaux devraient adopter la validation du courriel sur tous leurs serveurs Simple Mail Transfer Protocol (SMTP) (c'est-à-dire entrée, sortie, relais).

Traditionnellement, les serveurs de courriel Internet acceptaient des messages provenant de n'importe quelle source adressés à n'importe quelle destination. Malheureusement, au cours des années 1990, les polluposteurs ont commencé à utiliser les serveurs de courriel de façon abusive, si bien que les FSI ont dû reconfigurer les serveurs de manière à ce que seuls leurs propres utilisateurs puissent s'en servir pour envoyer des courriels. Les FSI peuvent avoir recours à différentes techniques pour reconnaître les courriels provenant de leurs propres utilisateurs. La technique la plus courante consiste à utiliser l'authentification SMTP (définie dans le Request for Comments 2554), selon laquelle l'expéditeur procède lui-même à l'authentification auprès du serveur de courriel, d'ordinaire en employant les mêmes nom d'utilisateur et mot de passe qui lui permettent d'accéder aux courriels entrants. De cette façon, chaque message est associé à un utilisateur en particulier.

Si l'on connaît la source des pourriels sortants, il sera possible de les bloquer.

9. Les avis de non-remise (NDN) ne devraient être envoyés que dans les cas de courriels légitimes.

Sur le plan technique, il n'est pas plus difficile d'indiquer une fausse adresse de retour dans un courriel que dans une lettre sur support papier. Par conséquent, la plupart des pourriels renferment maintenant une adresse invalide, si bien que les avis de non-remise seraient envoyés à l'utilisateur de bonne foi dont l'adresse a été employée et non au polluposteur. Les domaines dont le nom a été contrefait à grande échelle peuvent recevoir chaque jour de grandes quantités d'avis de non-remise se rapportant à des adresses contrefaites, ce qui constitue un inconvénient de taille pour les utilisateurs.

Il serait aussi possible de cesser complètement d'envoyer des avis de non-remise. Or, cette avenue n'est pas souhaitable, car les expéditeurs légitimes ne pourraient savoir s'ils ont mal tapé une adresse ou envoyé du courriel à une adresse désuète. Au lieu de cela, les exploitants de réseaux peuvent souvent configurer leur serveur de courriel de manière à ce qu'il rejette les courriels non délivrés au moment où l'hôte essaie de les expédier. Si cet hôte est un serveur de courriel légitime, il créera un avis de non-remise ou avisera l'expéditeur d'une autre façon. S'il s'agit d'un programme de pollupostage, le serveur de courriel n'en tiendra pas compte et ne créera aucun avis de non-remise. Les exploitants de réseaux peuvent aussi utiliser des filtres contre les pourriels et les virus pour les courriels non délivrés et envoyer des avis de non-remise uniquement dans le cas des courriels non considérés comme des pourriels ou des sources de virus.

Cette pratique exemplaire n'empêche pas les pourriels à proprement parler, mais elle permet de réduire les inconvénients subis par les utilisateurs dont l'adresse a été utilisée par les polluposteurs.

10. Les FSI et autres exploitants de réseaux devraient veiller à ce que tous les noms de domaine, les fichiers de systèmes de noms de domaine (DNS) et les fichiers d'enregistrement d'adresse IP applicables (WHOIS/SWIP/RWHOIS) soient maintenus à jour à l'aide de renseignements corrects, complets et courants. Ces renseignements devraient comprendre les points de contact responsables de résoudre les questions d'abus et inclure, sans toutefois s'y limiter, les adresses postales, les numéros de téléphone et les adresses de courriel.

Chaque domaine utilisé dans Internet (par exemple, **gc.ca** ou **exemple.com**) est enregistré auprès d'un registraire ou d'un groupe de registraires. Au moment de l'enregistrement, les propriétaires du domaine donnent leurs coordonnées, notamment leur nom, adresse postale, numéro de téléphone et adresse de courriel. Les registres donnent accès en totalité ou en partie aux renseignements sur les propriétaires des noms de domaine inscrits grâce à la base de données WHOIS. Une fois le nom de domaine inscrit, le propriétaire du domaine crée des fichiers de systèmes de noms de domaine (DNS), afin de diffuser à l'intention des internautes l'emplacement des serveurs de courriel, des serveurs Web et des autres serveurs réseau.

En outre, lorsqu'un réseau canadien a besoin d'une adresse IP pour son propre usage ou celui de ses clients, il l'obtient auprès d'un registre régional appelé « American Registry for Internet Numbers » (ARIN). Cette fois encore, le réseau fournit ses coordonnées au moment de l'enregistrement. S'il affecte par la suite à des réseaux clients une partie des adresses IP qui lui ont été attribuées, le réseau peut utiliser le fichier SWIP pour ajouter leurs coordonnées dans ARIN. Par ailleurs, ARIN exploite également une base de données WHOIS qui donne des renseignements sur les propriétaires inscrits des adresses IP attribuées. Les exploitants de réseaux peuvent aussi créer des entrées spéciales pour les systèmes de noms de domaine appelés « DNS inversé » ou « rDNS » pour documenter les noms de domaines attribués à chacune de leurs adresses IP.

Les données des fichiers DNS et WHOIS sont des outils essentiels pour retracer l'usage abusif d'Internet, y compris les pourriels. Comme il est facile de contrefaire les noms de domaine dans les courriels, la seule information fiable pour identifier la source d'un pourriel ou d'un message porteur d'un virus est l'adresse IP de l'hôte qui l'a envoyé. Grâce aux fichiers WHOIS et DNS inversés, le destinataire peut identifier la partie responsable de l'adresse IP pour autant que l'information obtenue soit exacte. Par conséquent, il est important que les exploitants de réseaux veillent à l'exactitude des renseignements fournis à la base de données WHOIS et les mettent à jour lorsque les coordonnées changent.

Cette pratique exemplaire pourrait non seulement aider à identifier les polluposteurs, mais aussi permettre aux utilisateurs légitimes de s'identifier.

11. Les FSI et autres exploitants de réseaux devraient veiller à ce que leurs adresses routables et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP. Tous les exploitants de réseau local d'entreprise (RLE) devraient se conformer au document Request for Comments (RFC) 1918 — « Address Allocation for Private Internets ». Les RLE, plus particulièrement, ne devraient pas utiliser l'espace IP enregistré globalement à quelqu'un d'autre ou l'espace IP non enregistré à quelqu'un, à titre d'espace IP privé.

Chaque réseau possède une série d'adresses IP attribuées aux ordinateurs qui en font partie. Dans la plupart des cas, les exploitants de réseaux déploient des efforts considérables pour éviter les doubles emplois et affecter chaque adresse IP à un ordinateur en particulier. C'est ce qui permet à tout autre ordinateur, n'importe où dans Internet, de communiquer avec cet appareil en utilisant l'adresse qui lui a été attribuée. Ces adresses à accès universel sont dites « routables » ou « visibles ».

Par ailleurs, il est possible de créer des réseaux privés en utilisant des adresses IP auxquelles on ne peut avoir accès à partir des autres réseaux Internet, lorsque la sécurité l'impose ou que le nombre d'ordinateurs sur le réseau est supérieur aux adresses IP routables disponibles. Par exemple, le FSI attribue généralement une seule adresse publique à l'utilisateur d'une ligne d'abonné numérique résidentielle ou d'un modem câble. L'utilisateur qui possède plusieurs ordinateurs raccordés à un réseau privé peut raccorder tous les appareils à ce réseau et utiliser un dispositif appelé « routeur » pour relier le réseau privé à Internet. Le routeur fait en sorte que les autres utilisateurs d'Internet voient alors le réseau privé comme un seul ordinateur doté d'une seule adresse IP publique. Les entreprises ont souvent recours à cette technique à grande échelle pour créer des réseaux privés sécurisés offrant un accès limité à l'Internet public.

Comme les ordinateurs d'un réseau privé ne sont pas reliés directement à Internet, il n'est pas nécessaire qu'ARIN attribue les adresses IP dans ce réseau. En 1996, le Request for Comments 1918 a défini les séries d'adresses IP à utiliser dans les réseaux privés. Depuis, tous les réseaux privés conçus selon les règles de l'art utilisent des adresses déterminées par cet appel de commentaires.

Malheureusement, certains réseaux privés utilisent des adresses non conformes au Request for Comments 1918, généralement des adresses que les gestionnaires de systèmes pensaient ne jamais voir attribuées à qui que ce soit. L'utilisation d'adresses non normalisées dans les réseaux privés pose des problèmes à ceux qui cherchent à retracer les cas d'usage abusif des réseaux; en effet, lorsqu'on examine un message ou les données de traçage du réseau, il est souvent impossible de déterminer si l'adresse non normalisée est utilisée dans un réseau privé. Qui plus est, dans les cas où l'adresse a été

attribuée à un autre utilisateur légitime, l'utilisation d'une adresse non normalisée peut lui faire porter le blâme.

Cette pratique exemplaire se rapporte à la recommandation 10 et sa mise en œuvre pourrait aider à dépister les polluposteurs. Elle offrirait aussi aux utilisateurs légitimes du courriel un moyen de s'identifier.

12. Les FSI et autres exploitants de réseaux devraient interdire l'envoi de courriels renfermant des en-têtes frauduleux ou contrefaits. L'en-tête de message devrait être exact et conforme aux documents RFC pertinents, notamment le RFC 822 et le RFC 2822, et les domaines de référence et les adresses IP devraient comporter des données d'enregistrement exactes et à jour.

Chaque fois qu'un serveur de courriel prend en charge un message, il ajoute au haut de ce message un en-tête permettant de retracer l'expéditeur. La série d'en-têtes qui figurent sur un message vise à documenter son parcours dans le système de courriel d'Internet. Comme chaque serveur ajoute simplement son en-tête aux mentions y figurant déjà, il n'est pas difficile pour les auteurs de virus ou les polluposteurs d'insérer des en-têtes contrefaits pour camoufler la source réelle du courriel. De plus, certains logiciels de courriel légitimes n'utilisent pas une présentation appropriée et produisent des en-têtes qui, sans être frauduleux, peuvent induire en erreur.

Les exploitants de réseaux connaissent la structure de leur réseau, et ils peuvent en tirer parti pour refuser les courriels qui comportent différents types d'en-têtes contrefaits. Par exemple, si un message a été envoyé à partir d'un ordinateur hôte qui a une adresse IP particulière dans un réseau, on peut présumer que tout en-tête de message faisant en sorte que le message semble provenir d'une autre source est contrefait.

Cette pratique exemplaire se rapporte à la recommandation 10 et sa mise en œuvre pourrait aider à dépister les polluposteurs. Elle offrirait aussi aux utilisateurs légitimes du courriel un moyen de s'identifier.

Références

Tous les appels de commentaires (Requests for Comments) sont diffusés en ligne (www.rfc-editor.org/rfc.html).

D. Crocker. RFC 822 — *Standard for the format of ARPA Internet text messages*, août 1982.

D. Karrenberg et coll. RFC 1918 — *Address Allocation for Private Internets*, février 1996.

J. Klensin (dir.). RFC 2821 — *Simple Mail Transfer Protocol*, avril 2001. (Mise à jour du RFC 821)

J. Myers. RFC 2554 — *SMTP Service Extension for Authentication*, mars 1999.

J. Postel. RFC 821 — *Simple Mail Transfer Protocol*, août 1982.

P. Resnick (dir.). RFC 2822 — *Internet Message Format*, avril 2001. (Mise à jour du RFC 821)