Messagerie, mode d'emploi

« *On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère*. »

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LEN)

Décembre 2011

Document destiné à l'usage exclusif des clients d'Azimut communication.

www.azimut.net

AZIMUT COMMUNICATION - SOLUTIONS INTERNET - BORNES INTERACTIVES
ZA Kerhoas, 5 rue de Bretagne 56260 LARMOR PLAGE -
Tel : 02.97.88.26.26 - Fax : 02.97.88.26.27 - www.azimut.net - azimut@azimut.net
Société au capital de 24 000 euros - SIREN : 394 280 697 - SIRET : 394 280 697 00043

Ce document a pour objectif de vous préciser quelques informations essentielles concernant l'usage de votre messagerie électronique.

- Comment ça marche ? :
- IMAP ou POP…Que choisir ?
- Comment configurer ma messagerie ?
- Comment utiliser le webmail Azimut ?
- Vous avez dit netiquette ?
- Et les arnaques ?
- Et les virus ?
- Glossaire

Comment ça marche ?

S'il parait simple et naturel d'envoyer et de recevoir des E-mail, derrière se cache un fonctionnement relativement complexe qui fait appel à des protocoles, des serveurs, des logiciels de messagerie, bref un grand nombre d'éléments interdépendants et nécessaires pour communiquer par courriel.

Lors de l'envoi d'un E-mail, le message est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire. Ces serveurs qui acheminent vos messages sont appelés **MTA** pour *Mail Transport Agent*.

Sur internet, les **MTA** communiquent entre-eux grâce au protocole **SMTP** ; Ils sont logiquement appelés **serveurs SMTP** (parfois *serveur de courrier sortant*). C'est grâce à eux que vous pouvez envoyer vos messages). Le servveur SMTP dépend de votre fournissseur d'accès (smtp.free.fr, smtp.orange.net…)

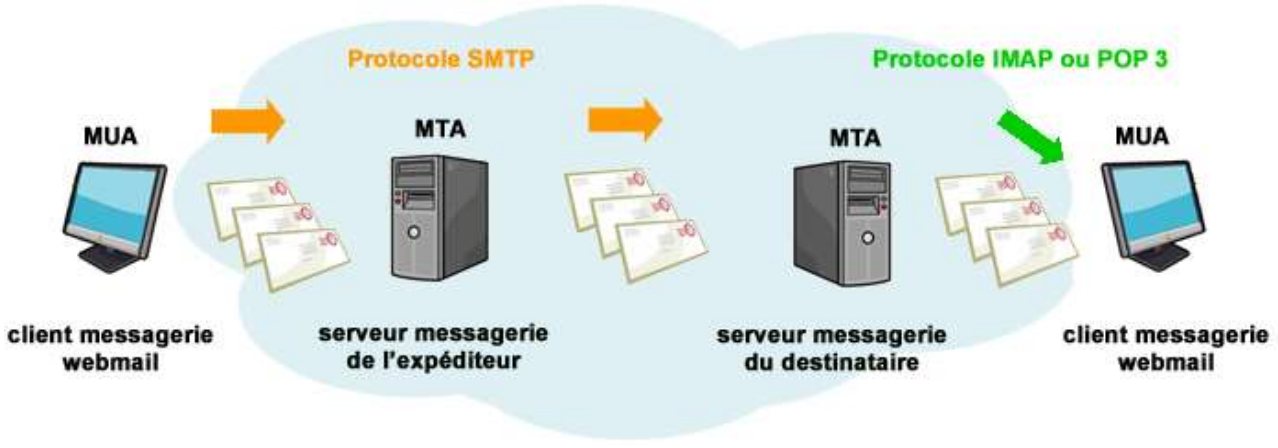
A l'autre bout de la chaîne, côté destinataire, votre message sera stocké sur un serveur entrant ou **MDA** pour *Mail Delivery Agent*. en attendant que l'utilisateur vienne le relever. Il existe deux principaux protocoles permettant de relever le courrier:

- le protocole POP3 (*Post Office Protocol*), permet de relever son courrier et de récupérer ses messages sur son poste de travail (ordinateur).
- le protocole IMAP (*Internet Message Aess Protocol*), permet une synchronisation de l'état des courriers (lu, supprimé, déplacé) entre plusieurs clients de messagerie. Avec le protocole IMAP une copie de tous les messages est conservée sur le serveur afin de pouvoir assurer la synchronisation.

Les serveurs de courrier entrant sont appelés **serveurs POP** ou **serveurs IMAP**, selon le protocole utilisé.

La relève du courrier se fait grâce à un logiciel appelé **MUA** (*Mail User Agent*). Le MUA est un logiciel installé sur le terminal (ordinateur,tablettes, smartphone)…) de l'utilisateur, on parle de **client de messagerie** (par exemple *Mozilla Thunderbird*, *Microsoft Outlook*, *Eudora Mail*, *Incredimail* ou *Lotus Notes*).

Si vous consultez votre courrier électronique directement en ligne à partir d'une interface web on parle alors de **webmail**.



MUA	MTA	MDA
Client messagerie	Serveur sortant	Serveur entrant
	SMTP	POP/IMAP
Mozilla Thunderbird, *Microsoft Outlook*, *Eudora Mail*, *Incredimail* ou *Lotus Notes*…	Dépend de votre fournisseur d'accès internet ou de votre fournisseur de messagerie	

IMAP ou POP … Que choisir ?

Pour envoyer un courriel, il faut utiliser le protocole SMTP. Par contre pour consulter/relever/lire ses mails 2 options (ou protocoles) sont disponibles : l'IMAP ou le POP. Ce choix n'est pas anodin d'autant qu'une gestion rigoureuse de notre serveur de messagerie impose un quota '1 G° de stockage par compte mail. Dans le cas de l'option compte POP, cela n'a pas d'incidence sur l'utilisation de votre messagerie électronique. Par compte, cela impacte la gestion de vos mails en cas de fonctionnement en mode IMAP.

Le POP ou POP3 a été conçu pour permettre le traitement hors-ligne du courrier électronique. Cela signifie que lorsque vous connectez à votre serveur de messagerie votre client messagerie (*Outlook, Thunderbird*…) ,vous récupérez vos messages sur votre ordinateur où ils sont stockés. De ce fait vos messages ne sont plus sur le serveur. Vous pouvez donc consulter et classer vos anciens messages sans pour autant être connecté.

La philosophie de l'**IMAP** est différente. Le principe est de gérer et conserver ses messages sur le serveur. La gestion se fait donc en ligne ce qui implique d'être connecté pour accéder à sa messagerie. L'avantage est de s'affranchir d'un poste de travail dédié. L'inconvénient de stocker ses messages sur le serveur, est la gestion des ressources d'où la mise en place de quotas pour éviter les abus. Des options d'augmentation de capacité de stockage sont possibles, mais cela engendre des coûts.
Rappel : L'ouverture de compte mail est gratuite. Pour conserver ce service à l'ensemble de nos clients, nous avons pris la décision de mettre en place des quotas. Cela concerne essentiellement les utilisateurs de compte IMAP.

	Avantages	**Inconvénient**
POP	Le POP est simple et efficace. Gestion des messages en local après téléchargement, donc recherches et tris plus rapides et efficaces. Pris en charge dans de nombreux clients email. Utilisation minimale des ressources du serveur.	Gestion des sauvegardes par l'utilisateur
IMAP	L'IMAP permet une gestion simplifiée de la messagerie en cas de mobilité de l'utilisateur (gestion des dossiers et messages sur le serveur). Il est plus facile de changer de client de messagerie (aucun message à transférer, etc.) Il peut accéder à des boîtes aux lettres multiples et les gérer..	Il faut gérer son espace disque sur le serveur. Certains clients email sont plutôt lents pour récupérer des dossiers volumineux. Moins rapide pour les recherches dans les messages sur le serveur.

Comment configurer ma messagerie ?

Notre nouveau serveur de messagerie intègre un mode sécurisé (SSL). Vous avez donc le choix de diffuser vos messages en texte clair ou chiffré. Attention, la sécurisation des messages ne concerne uniquement que vos comptes mails créés sur notre serveur de messagerie. Cela ne concerne donc pas vos boites E-mails type free, gmail, yahoo.

Si les clients messagerie du marché proposent des fonctionnalités différentes, tous, en règle générale, vont vous demander des éléments communs pour paramétrer votre boite et pouvoir ainsi recevoir et expédier vos messages. Ainsi sur un même client de messagerie vous avez la possibilité d'activer plusieurs comptes qui ne sont pas forcément du même opérateur (Boite mail *Azimut, Gmail, Free, Orange*…). Cela signifie qu'en fonction du compte utilisé, il faudra modifier votre paramètre SMTP pour pouvoir envoyer vos messages, sinon cela ne marche pas. Exemple : maboite@free.fr > smtp.free.fr, maboite@orange.fr > smtp.orange.fr.

Nota : Ce qui est vrai pour les clients messagerie de vos ordinateurs, l'est aussi pour le paramétrage de comptes sur votre smartphone. Cependant suivant les logiciels, les éditeurs, les marques, il est possible que le processus de configuration diffère. Nous vous conseillons de bien étudier la notice. Nous sommes cependant à votre service pour vous aider dans ces opérations qui simples de prime abord, se révèlent parfois complexes.

Les paramètres demandés :

- Nom du compte ou nom utilisteur (votre boite mail)
- Votre mot de passe (fourni par votre prestataire)
- Votre serveur POP (fourni par votre prestaire)
- Votre SMTP (dépend de votre fournisseur d'accès internet ou de messagerie)
- Le port (cela permet de diriger les informations en provenance d'un serveur vers une application donnée. Celui du serveur POP est différent de celui du SMTP par exemple)

Configuration en mode pop classique

Le mode classique est adapté pour les postes de bureau connectés à un réseau filaire.

Nom d'utilisateur : votre adresse mail
Mot de passe : xxx (fourni par Azimut)
Serveur pop : mail.mon_nom_de_domaine (ex : mail.azimut.net) / Port 110 (par défaut)
SMTP : **SMTP.votre_fournisseur_accès_internet (ex :SMTP.orange.fr) / Port 25 (par défaut)**

Configuration en mode pop3 sécurisé

Le mode sécurisé est adapté pour les postes mobiles (portable) ayant l'habitude de se connecter à des réseaux wifi non chiffrés (wifi public par exemple).

Nom d'utilisateur : votre adresse mail
Mot de passe : xxx (fourni par Azimut)
Serveur pop : securimail.azimut.net / port 995 (SSL/TLS) ou port 110 (STARTTLS)
SMTP : securimail.azimut.net / port 25 (STARTTLS) - port 465 (SSL/TLS) ou port 587 (STARTTLS

ATTENTION : Le choix du port en mode sécurisé dépendra de votre opérateur de connexion internet ou FAI (fournisseur d'accès internet) ainsi que des logiciels de sécurité (antivirus et firewall) installés sur le poste ou sur votre réseau. En effet, certains opérateurs ne permettront pas une connexion sur tel ou tel port, et certains logiciels de sécurité risquent de vous alerter lors de connexion chiffrée qu'ils ne pourront pas analyser.

En mode pop3, pensez à configurer les logiciels de messagerie pour effacer les messages sur le serveurs :

Thunderbird : Dans "paramètres serveur", ne pas cocher la case "Laisser les messages sur le serveur ou alors en spécifiant un temps de conservation
Outlook 2007 / outlook 2010 : Dans "paramètres supplémentaires"/"Options avancées" ne pas cocher la case « Laisser un exemplaires des messages sur le serveur » ou alors en spécifiant un temps de conservation
Windows live mail : Attention, le paramétrage par défaut de Windows Live Mail est de conserver les messages sur le serveur. Dans "propriété du compte"/"avancé" ne pas cocher la case "Conserver une copier des messages sur le serveur ou alors en spécifiant un temps de conservation
Mac OS mail : Attention, le paramétrage par défaut de Mac OS Mail est de conserver les messages sur le serveur durant 1 semaine.Dans "propriété du compte"/"Avancé" Cocher la case "Après récupération, supprimer la copie du serveur" et sélectionner "Immédiatement"

Configuration en mode IMAP classique

Rappel : Le principe de la consultation des messages en IMAP est de conserver ces messages sur le serveur et de synchroniser le statut (lu, non lu) et l'organisation (rangement dans des dossiers) des messages entre votre poste et le serveur. Les messages sont stockés le serveur, sont marqués comme lu ou non, mais ne sont pas classés dans des dossiers suivant votre usage.
Le mode IMAP est particulièrement adapté pour les boites E-mails relevées par plusieurs personnes ou sur plusieurs poste (poste fixe de bureau, portable et téléphone). La connexion au serveur de messagerie est nécessaire pour le bon fonctionnement.

Attention, en mode IMAP, les messages, il faut faire attention à la consommation du quota d'espace disque. Il est fixé par défaut à 1Go. Cela implique qu'il faut « nettoyer » (supprimer des messages) sa boite E-mail de temps en temps pour éviter une saturation. Une boite pleine ne peut plus recevoir de messages !

Nom d'utilisateur : votre adresse mail
Mot de passe : xxx (fourni par Azimut)
Serveur IMAP : mail.mon_nom_de_domaine (ex : mail.azimut.net) / Port 143 (par défaut)
SMTP : **SMTP.votre_fournisseur_accès_internet (ex :SMTP.orange.fr) / Port 25 (par défaut)**

Configuration en mode IMAP sécurisé

Nom d'utilisateur : votre adresse mail
Mot de passe : xxx (fourni par Azimut)
Serveur pop : securimail.azimut.net - port 143 (STARTTLS) - port 993 (SSL/TLS)
SMTP : securimail.azimut.net / port 25 (STARTTLS) - port 465 (SSL/TLS) ou port 587 (STARTTLS

ATTENTION : Le choix du port en mode sécurisé dépendra de votre opérateur de connexion internet ou FAI (fournisseur d'accès internet) ainsi que des logiciels de sécurité (antivirus et firewall) installés sur le poste ou sur le réseau. En effet, certains opérateurs ne permettront pas une connexion sur tel ou tel port, et certains logiciels de sécurité risquent de vous alerter lors de connexion chiffrée qu'ils ne pourront pas analyser.

Dans le cas d'une utilisation nomade avec une connexion à un WIFI public, les règles de sécurité des réseaux peuvent varier. Cela signifie que l'envoi d'un mail sur un port choisi peut fonctionner sur un réseau wifi et pas un autre. Pour pallier à ce problème, il est préférable pour l'envoi des messages de se connecter uniquement sur le réseau de l'**opérateu**r en **mode 3G** ou sur des réseaux WIFI connus.

Si vous utilisez notre serveur SMTP une identification vous sera demandée à savoir votre adresse E-mail et votre mot de passe de messagerie.

Comment utiliser le webmail Azimut ?

Défintion Wikipedia : Le webmail est un logiciel de messagerie hébergé sur le web. Il permet de consulter directement les messages sur le serveur. Seuls les messages qui n'ont pas été supprimés sont visibles

Notre serveur de messagerie vous propose d'accéder à un Webmail (www.extrazimut.net , rubrique « Webmail ») . Bien entendu ce webmail ne concerne que les boites E-mails qui ont été créées sur notre serveur de messagerie.

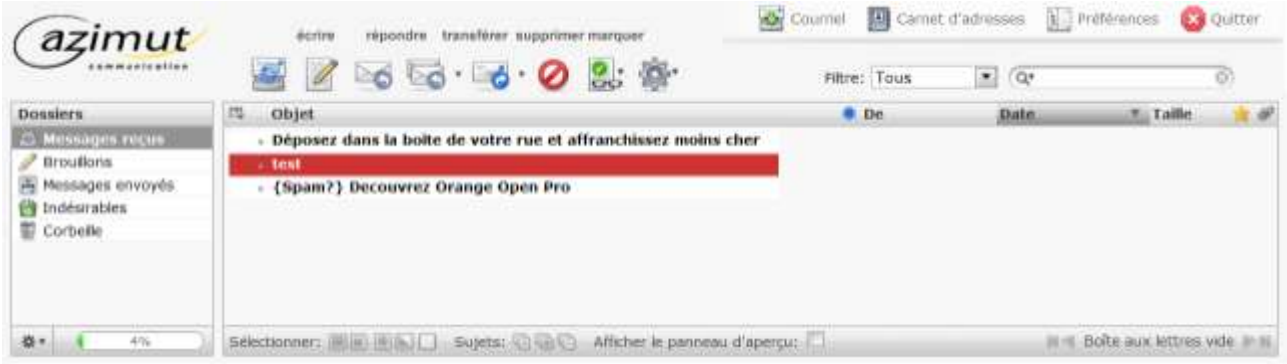
Dans un souci de protection du contenu de vos messages, la connexion à notre webmail se fait désormais automatiquement en mode sécurisé.

Le Webmail d'Azimut vous permet :

- De consulter vos messages
- De classer vos messages
- De supprimer les messages indésirables
- De transférer vos messages
- De constituer un annuaire
- D'écrire à vos contacts (avec ou sans pièce jointe).

L'utilisation du Webmail est pratique lors de vos déplacements. Vos messages restent visibles tant que vous n'utilisez pas votre client messagerie configuré en mode POP. Dans ce cas, vos messages sont transférés sur votre terminal

.



Les préférences

Notre webmail vous permet de gérer différents paramètres afin d'en optimiser son utilisation :

Paramétrer votre webmail

- Interface utilisateur : Sélection de la langue et du nombre de réponses par page
- Vue du courrier : Gestion des aperçus et des notifications
- Ecriture des messages : Vérification de l'orthographe, gestion des brouillons, des signatures…
- Affichage des images : Gestion de la visualisation des messages
- Carnet d'adresses : Autorise ou non, l'ajout de contacts
- Dossiers spéciaux : Brouillons, Messages envoyés, Indésirables, Corbeille
- Préférences du serveur : Gestion de la suppression des messages, de la corbeille

Gérez vos dossiers

Cette fonctionnalité vous permet de gérer vos dossiers (Création, suppression, ajout de sous-dossiers) ainsi que le mode d'affichage des listes.

Gérer vos identités

Plusieurs personnes peuvent utiliser un même compte de messagerie. Cette fonctionnalité permet de paramétrer l'identité d'un utilisateur en fonction des besoins. Très pratique pour votre destinataire qui peut ainsi identifier qui lui répond.

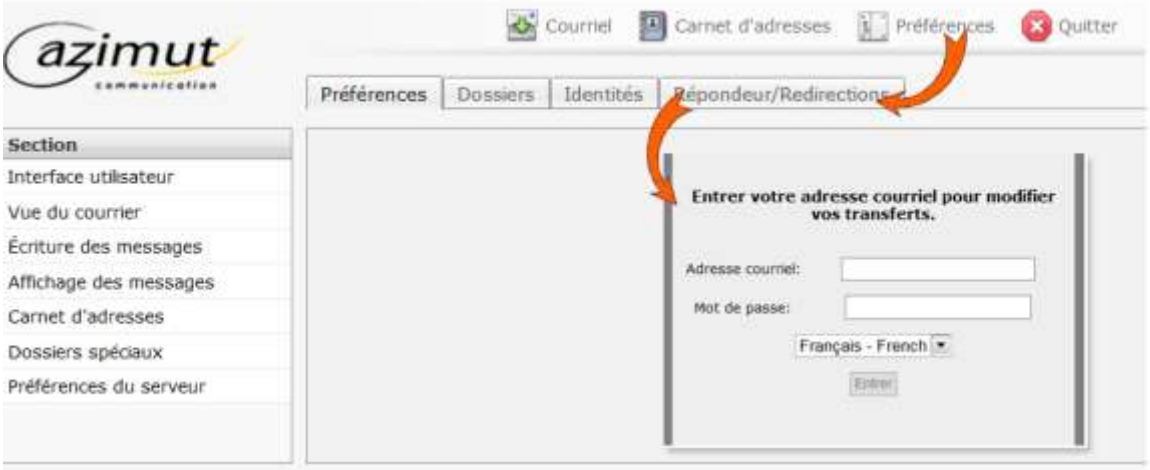
Gestion du message d'absence / répondeur automatique

Cette fonction permet d'envoyer automatiquement une réponse à tous les messages que vous recevez via votre messagerie électronique. En cas d'absence (pour congés par exemple), vous avez le possibilité de personnaliser un message et d'informer vos interlocuteurs de vos disponibilités.

Procédure

Cliquez sur l'onglet « préférences » puis sur « Répondeur/Redirection ».

Vous devrez de nouveau vous identifier avec votre adresse mail et mot de passe.



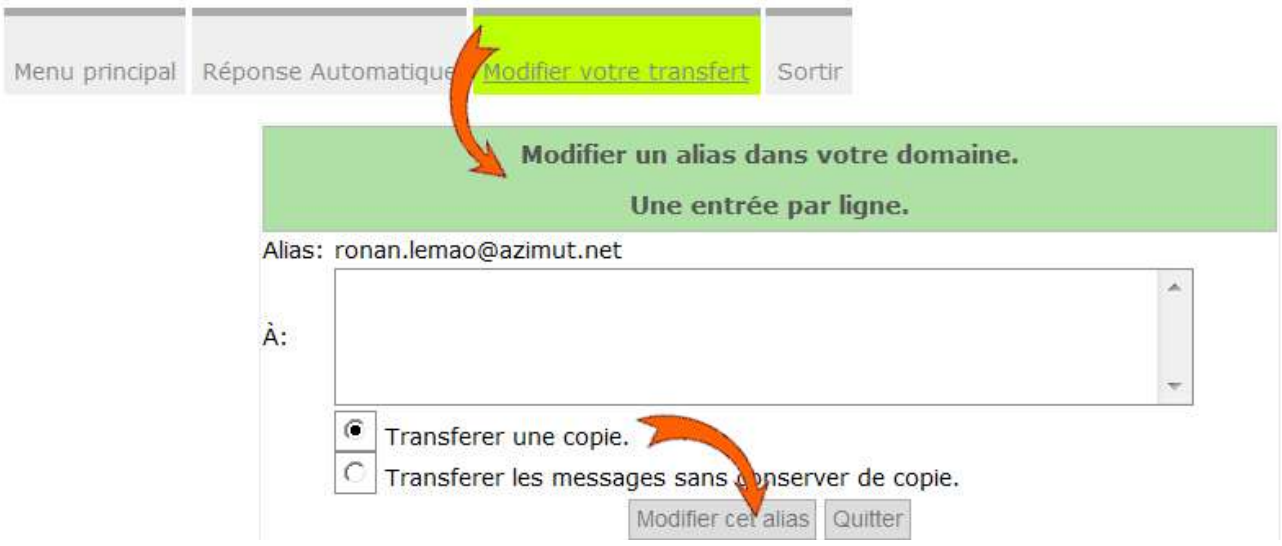
Cliquez sur "Réponse automatique"
.

Vous pouvez alors noter votre message
Pour le valider, cliquez du le bouton « Absence », cela va activer automatiquement ce message.
Pour désactiver ce message d'absence automatique, il faut se reconnecter à l'application et cliquer sur sur le bouton "De retour"

Gestion des transferts de messages

La procédure d'accès est identique à celle du message d'absence
Connexion webmail > préférences > Répondeur/Redirection> Identification
Cliquer sur "Modifier votre transfert".

Dans le champ "à", renseignez les adresses des destinataires (une adresse par ligne)
Si vous voulez conserver les messages sur cette boite, sélectionnez "Transferer une copie".
Si vous ne voulez pas conserver les messages sur cette boite, sélectionner "Transferer les messages sans conserver de copie".



Vous avez dit netiquette ?

Attenition à ce que vous écrivez ! : Un e-mail, ça s'écrit vite, ça part vite, ça arrive vite, et ça peut faire beaucoup de dégats. Relisez les courriers sensibles plutôt deux fois qu'une.

Réflechissez à deux fois avant de forwarder un e-mail : Vous vous apprêtez à faire suivre un e-mail. Mais avez-vous la permission de l'auteur ? Car divulguer à un tiers le contenu d'une conversation privée peut être dommageable...Attention au contenu et messages inclus de la mail qui vous forwardez !

N'envoyer le courrier électronique qu'aux personnes concernées - Il est déplacé, et désagréable pour les destinataires, de transmettre du courrier électronique à n'importe qui. Les destinataires perdent notamment un temps précieux à trier entre les messages qui les concernent vraiment et ceux qui ont peu ou aucun intérêt pour eux.

Soignez vos messages : Même si le ton d'un e-mail est moins formel que celui d'une lettre écrite, efforcez-vous de respecter les règles d'orthographe et de grammaire. N'oubliez pas non plus la politesse. Les expressions simples, du type "Bien à vous" ou "Cordialement" ont la cote.

Évitez les mots tout en majuscules : L'utilisation des majuscules dans les courriels équivaut à CRIER. Mieux vaut donc éviter d'écrire des mots complets en majuscules.

Évitez les informations confidentielles : N'envoyez jamais d'information confidentielle par e-mail, en particulier votre numéro de carte bancaire, vos codes secrets et mots de passe, sauf s'il s'agit d'un e-mail sécurisé

Indiquer clairement le sujet du message dans la zone « Objet » (ou « Sujet ») Ceci est particulièrement important pour le destinataire. Il sera d'autant plus facile pour le destinataire de distinguer dans l'ensemble des courriers qu'il reçoit ceux qui sont prioritaires de ceux qui le sont moins si le sujet du message est explicite.

Être bref et bien situer le contexte du message. Pour être lu et bien compris, il est préférable d'utiliser des phrases courtes et précises. Si le message est long, le diviser en plusieurs paragraphes en facilite la lecture. Un texte précis et bien structuré permet d'éviter les malentendus ou une mauvaise interprétation.

S'il faut attacher des documents au message, pensez aux destinataires Le destinataire d'un fichier attaché ne possède pas forcément les logiciels permettant de le lire. Assurez-vous que le fichier est enregistré dans un format décodable par la plupart des logiciels courants. (ex. .doc plutôt qur .docx). Par ailleurs, faites attention à la taille des fichiers attachés. Plus la taille est importante, plus le temps de transmission et de réception sera long. Avant l'envoi d'un message sensé contenir une pièce jointe, veillez à ce que la pièce jointe soit bien présente !

S'assurer de bien s'identifier et de laisser des coordonnées à la fin du message. Pensez à laisser votre signature au bas des messages, mais sans prendre trop de place (4 ou 5 lignes au maximum), en précisant par exemple votre fonction, votre entité de rattachement. Les coordonnées téléphoniques peuvent être utiles si un de vos destinataires cherchent à vous joindre rapidement. Evitez l'usage d'une image incluant vos coordonnées comme signature. Par défaut elle ne s'affiche pas.

Prenez garde aux envois en nombre : Si vous devez envoyer un e-mail à un nombre important de destinataires, placez les adresses dans le champ *copie cachée* (Bcc: ou Cci:). De cette façon, chaque destinataire n'aura pas connaissance de la liste des destinataires.

Définissez des priorités aux messages : Si nécessaire, attribuez une priorité (importance) au message que vous envoyez. Attention: si vous envoyez tous vos courriels en "haute priorité", vous risquez de ne plus être crédible. De toutes façons cela n'a aucun impact sur le serveur qui ne traitera pas en priorité vos messages prioritaires.

Utilisez le mail avec parcimonie : Ne noyez pas vos correspondants sous les e-mails. Limitez autant que possible le nombre de messages que vous envoyez.

Et les arnaques ?

Le scam

Le « scam » (« ruse » en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est issue du Nigéria, ce qui lui vaut également l'appellation « 419 » en référence à l'article du code pénal nigérian réprimant ce type de pratique. L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds. En répondant à un message de type scam, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euros s'il mord à l'hameçon et même la vie dans certains cas.
En effet, deux cas de figures se présentent :
Soit les échanges avec l'escroc se font virtuellement auquel cas celui-ci va envoyer quelques « documents officiels » pour rassurer sa victime et petit à petit lui demander d'avancer des frais pour des honoraires d'avocats, puis des frais de douanes, des frais de banque, etc.
Soit la victime accepte, sous pression du cyberbandit, de se rendre dans le pays avec la somme en liquide auquel cas elle devra payer des frais pour pouvoir rester dans le pays, payer des frais de banque, soudoyer des hommes d'affaires, et ainsi de suite.
Dans le meilleur des cas la victime rentre chez elle en avion délestée d'une somme d'argent non négligeable, dans le pire scénario plus personne ne la revoit...

Le phishing

Le phishing (contraction des mots anglais « fishing », en français pêche, et « phreaking », désignant le piratage de lignes téléphoniques), traduit parfois en « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.
La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.
Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.
Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque.
Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).
Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

Loterie internationale

Vous recevez un courrier électronique indiquant que vous êtes l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euros. Pour empocher le pactole il suffit de répondre à ce courrier.
Après une mise en confiance et quelques échanges de courriers, éventuellement avec des pièces jointes représentant des papiers attestant que vous êtes bien le vainqueur, votre interlocuteur vous expliquera que pour pouvoir toucher ladite somme, il faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses et variées, etc.
C'est de cette façon que ces cybertruands arrivent à extorquer des milliers d'euros à des internautes dupes de cette supercherie.

Et les virus ?

Un virus est un programme dont le but est de se reproduire. Sa technique est de s'accrocher à un programme existant, à la manière d'un parasite.

Un ver (ou worm en anglais) est également un programme autoreproducteur. Mais à la différence du virus, il se suffit à lui même : il n'a pas besoin d'un programme hôte pour se reproduire. La méthode la plus courante de propagation des vers est l'envoi de courriers électroniques avec copie du ver en pièce jointe.
Un troyen ou cheval de Troie (ou trojan en anglais) est un programme qui permet de prendre le controle à distance de votre machine et de lui faire exécuter des commandes à votre insu (vol des mots de passe, accès à distance aux ressources de la machine, destruction de données, etc.). Il n'a pas de facultés autoreproductrices.
Dans le cas des virus et des vers, l'objectif principal est la reproduction. Dans le cas d'un troyen, c'est la prise de commande de l'ordinateur. Mais même si ces 3 entités ne sont pas destructrices, elles consomment des ressources système de votre ordinateur (microprocesseur, espace disque, etc.) et causent forcément quelques désagréments.

Où se cachent les virus ?

- dans les fichiers attachés
- à l'intérieur même du mail
- dans un lien

Comment se protéger ?

- Méfiez-vous des pièces attachées
- Méfiez vous des messages dont vous ne connaissez pas l'expéditeur
- Augmentez le niveau de sécurité de votre navigateur
- Augmentez le niveau de sécurité de votre client messagerie
- Installez un antivirus

Glossaire

Alias Adresse e-mail qui renvoie vers une autre adresse e-mail. Annexe Voir Pièce jointe.
Arobase Nom français du signe @, ou "a commercial", utilisé comme séparateur dans les adresses électroniques.
ASCII American Standard Code for Information Interchange La plupart des fichiers textes sont sauvés au format ASCII (prononcez aski). Mais ASCII est un peu plus qu'un format de texte, c'est un standard développé par l'American National Standards Institute (ANSI), pour définir comment les ordinateurs écrivent et lisent les caractères. Le code ASCII comprend 128 caractères, incluant lettres, chiffres, signes de ponctuation et codes de contrôle (comme le caractère qui marque la fin d'une ligne). Chaque lettre ou caractère est représenté par un nombre : le A majuscule est par exemple le numéro 65 et le z minuscule le numéro 122. La plupart des systèmes utilisent le code ASCII standard.
Attachement Anglicisme. Voir Pièce jointe.
BAL Boîte aux lettres.
Bcc Blind Carbon Copy Copie d'un message envoyé à un destinataire sans que les autres destinataires ne s'en aperçoivent. Equivalent français : Cci (copie carbone invisible). Voir aussi Cc
Binette Voir smiley.
BinHex BINary HEXadecimal Méthode de conversion pour les fichiers binaires en ASCII, couramment utilisé chez les utilisateurs de Mac. Technique autrefois nécessaire lorsque les logiciels de messagerie ne supportaient pas le format MIME.
Body Voir corps.
Boîte POP Boîte e-mail pouvant être relevée avec un logiciel de messagerie, selon le protocole POP.
Bounce En anglais : rebondir Retour d'un e-mail à son expéditeur, suite à un disfonctionnement du réseau ou une erreur (du type utilisateur inconnu). Certains logiciels de lutte contre le spam émettent de faux bounces pour faire croire que votre adresse n'existe plus.
BulkMailer Logiciel servant à envoyer de grosses quantités de courrier électronique, généralement pour spammer.
Canular Syn. : hoax Faux message alarmant, ayant pour but la désinformation. Par défaut, un canular n'est pas dangereux pour votre ordinateur, mais peut être très gênant pour les serveurs de mails du fait qu'il vous est demandé de colporter vous-même la fausse information à tous vos contacts.
Cc Carbon copy, Courtesy copy ou Copie carbone Copie d'un courrier électronique envoyé à un ou plusieurs destinataires, différents des destinataires principaux.
Cci Copie carbone invisible Copie d'un message envoyé à un destinataire sans que les autres destinataires ne s'en aperçoivent. On dit aussi copie cachée. Équivalent anglais : Bcc (Blind carbon copy). Voir aussi Cc
Cheval de Troie Voir troyen.
CNIL Commission Nationale de l'Informatique et des Libertés Autorité administrative indépendante, veillant au respect des lois françaises concernant l'informatique, en particulier celles concernant la légalité et l'utilisation des fichiers nominatifs (loi Informatique et Libertés du 6 janvier 1978).
Corps . Partie principale d'un courrier électronique, située après les en-têtes. Il comprend le contenu du mail.
Courriel :Courrier électronique.
Compte POP voir boîte POP
DNSBL ou DNS-bl DNS Providers Blacklist Liste noire de domaines utilisés par les spammers. Voir aussi RBL
DSN Delivery Status Notification Avis de remise ou de non remise d'un courrier électronique (accusé de réception).
E-mailing En français : publipostage électronique Envoi massif d'e-mails, personnalisés ou non, à une liste de destinataires.
Emoticon ou Emoticône Voir smiley.
En-tête(s) Syn. : header Partie du courrier électronique qui contient les informations nécessaires à la gestion du message : expéditeur, destinataire, date d'envoi, etc. ... On utilise aussi le terme anglais header.
ESMTP Extended Simple Mail Transfer Protocol Extension du protocole SMTP, intégrant les extensions MIME (Multipurpose Internet Mail Extensions) et DSN (Delivery Status Notification) . Espiogiciel, espiongiciel Voir spyware.
FAE Fournisseur d'Adresses Électroniques : service qui propose des boîtes aux lettres électroniques (service de mail gratuit, hébergeur professionnel, fournisseur d'accès à Internet).

FAI Fournisseur d'Accès Internet (provider ou ISP en anglais).
FAQ Frequently asked questions ou Foire aux questions Liste des questions les plus fréquemment posées par les utilisateurs sur un sujet, accompagnées des réponses correspondantes.
Fichier attaché Voir Pièce jointe.
Fichier joint Voir Pièce jointe. Ftp-mail ou FTP par mail Téléchargement de fichiers par courrier électronique.
Header Voir en-tête.
Hoax Voir canular.
Identifiant En anglais : login Chaîne de caractère permettant une identification auprès d'un serveur. En matière de courrier électronique, l'identifiant est généralement la première partie de l'adresse e-mail, située avant le signe @. L'identifiant est souvent lié à un mot de passe.
IMAP Internet Message Access Protocol IMAP est un protocole d'accès aux boîtes à lettres électroniques, tout comme l'est POP. IMAP offre cependant davantage d'options que POP, comme la possibilité de ne charger seulement que les entêtes des courriers ou de gérer des boîtes aux lettres multi usagers.
Imprimable guillemeté Voir Quoted printable.
Junk mail Mail non sollicité. Voir spam.
Kerberos Système d'authentification réseau (basé sur des mots de passe) permettant par exemple aux utilisateurs de se connecter sur un serveur Windows 2000 et avoir accès à toutes les ressources réseau. Kerberos est pris en charge par quelques logiciels de messagerie dont Eudora.
Lidie Abréviation de Liste de diffusion.
Liste de diffusion 1. Liste d'adresses e-mail de personnes à qui sera envoyé un courrier électronique. 2. Méthode de diffusion d'information, dans laquelle les abonnés de la liste peuvent envoyer des messages qui seront diffusés aux autres.
Liste blanche liste reprenant les exceptions pour lesquelles la transmission du courrier se fait sans traitement anti-virus, anti-pourriel
Liste noire liste reprenant les exceptions pour lesquelles le courrier est directement rejeté ou marqué sans traitement anti-virus, anti-pourriel.
Liste grise greylisting mécanisme qui refuse les messages lors d'une première présentation et les accepte lors de leur présentation suivante.
Logiciel de messagerie Logiciel permettant d'envoyer, de recevoir et de gérer le courrier électronique. Les logiciels de messagerie les plus populaires sont Outlook Express et Outlook. Login Voir Identifiant.
Mailbombing Action de remplir une boîte à lettres électronique d'une très grande quantité de messages sans intérêt, dans le seul but de nuire.
Mailer Voir logiciel de messagerie.
Mailing list Voir liste de diffusion.
MAPI Mail Application Programming Interface Ensemble de fonctions logicielles permettant un pilotage (ou une programmation) des applications de courrier électronique. Ces fonctions permettent par exemple d'établir des liens entre le logiciel de messagerie d'une part et des logiciels comme Word ou Palm Desktop d'autre part.
Messagerie POP Voir boîte POP.
MIME Multipurpose Internet Mail Extensions. Mécanisme de codage d'informations permettant la transmission de documents multimédia entre deux machines s'appuyant sur des systèmes d'exploitation semblables ou distincts
MTA : Mail Transfer Agent (Agent de transport de courrier - voir aussi mail transport). Logiciel de serveur pour la vérification d'adresses de messages de courrier électronique et leur retransmission à une adresse locale du réseau ou sur Internet (sendmail, postfix...).
MUA, User Agent : Mail User Agent (agent de courrier utilisateur - voir aussi user agent). Logiciel client pour la composition et l'envoi de messages de courrier électronique (Eudora, Thunderbird, Evolution, Netscape Messenger, Outlook Express...).
Mail Transport L'office postal. Généralement un programme chargé de l'acheminement et de la distribution du courrier (sendmail, smail, MMDF, etc.).
Multi-pop Syn. : multi comptes Se dit d'un logiciel de messagerie capable de relever plusieurs boîtes aux lettres (selon le protocole POP). Aujourd'hui, la plupart des logiciels sont multi pop. Voir aussi POP
Multiè-comptes Voir multi pop.
Netiquette De network (brit.) et étiquette (fr.) Ensemble non officiel de règles de savoir-vivre sur les réseaux informatiques et donc sur Internet. Ces conventions, reconnues par tous, sont fondées autant sur la politesse et le respect d'autrui que sur les lois en vigueur. La Netiquette a été définie par l'IETF dans la RFC 1855. Newsletter Lettre d'information envoyée par e-mail à un certain nombre d'abonnés. O Pas de définition pour cette lettre
Pièce attachée Voir Pièce jointe.

Pièce jointe Syn : fichier joint, fichier attaché, pièce attachée, attachement Fichier (document Word, image, fichier MP3, etc.) joint à un courrier électronique. Ce fichier est encodé (généralement au format MIME) pour pouvoir être envoyé.

POP Post Office Protocol Protocole d'accès standard aux boîtes aux lettres électroniques. POP permet de se connecter au serveur qui stocke les messages, de proposer le login et le mot de passe, de lister les messages en présence et de les charger sur le disque local. Il permet enfin de détruire les courriers sur le serveur. La version courante de POP est POP3.
POP before SMTP Opération qui consiste à authentifier un usager via une consultation du serveur POP, pour lui autoriser dans la foulée l'utilisation du serveur SMTP.
QP Abréviation de Quoted printable. Quoted printable Technique de codage des caractères 8 bits en ASCII 7 bits, consistant à remplacer le caractère par son indice dans la table ASCII. « é » est par exemple remplacé par « =E9 ». Elle permet de faire passer les accents dans le courrier électronique.
RBL Realtime Blackhole List Liste noire de serveurs utilisés pour le spam. Voir aussi DNS BL Remailer Ré expéditeur anonyme. Service de courrier électronique permettant à un internaute d'expédier ses messages sans dévoiler son identité.

RFC Request for Comments Série de documents techniques, définissant les standards Internet.
Scam Arnaque par e-mail
Serveur de courrier entrant Voir serveur POP.
Serveur de courrier sortant Voir serveur SMTP. Serveur POP Serveur qui gère la relève du courrier électronique, également appelé serveur de courrier entrant. Son nom est généralement du type : mail.bidule.fr
Smiley Syn : binette, souriard, émoticon, émoticône, trombine Combinaison de caractères (par exemple ";-)"), qui permet de mettre de l'intonation dans un mail et d'ajouter nuances ou précisions aux propos.
Serveur SMTP Serveur qui permet l'envoi et la circulation du courrier électronique. Au niveau des logiciels de messagerie, il est également appelé serveur de courrier sortant. Son nom alors est généralement du type : mail.bidule.fr ou smtp.bidule.fr Voir aussi : SMTP
SMTP Simple Mail Transfer Protocol Protocole qui régule les échanges de courrier électronique, c'est à dire qui gère tout ce qui se passe entre deux serveurs de courrier. En gros, SMTP, c'est l'équivalent du service postal sur Internet. Voir aussi : serveur SMTP
Souriard Voir smiley.
Spam Syn. : spamming, polluriel, pourriel, courrier rebut, junk mail ou UCE (Unsollicited Commercial E-Mail). Message non sollicité, de type commercial (publicité) ou non (tracts).
Spyware Logiciel espion - Syn. : espiogiciel, espiongiciel Logiciel ou partie de logiciel qui transmet des informations sur l'utilisateur ou ses habitudes à son insu. Les annonceurs publicitaires sont généralement les destinataires de ces informations.
SSL Anglais : Secure sockets Layers Technologie de chiffrement des données. Elle est notamment utilisée par les sites Web, pour le commerce en ligne notamment.
Trojan Voir troyen. Trombine Voir smiley.
Troyen Syn. : cheval de Troie, trojan Programme qui permet de prendre le contrôle à distance de votre machine et de lui faire exécuter des commandes à votre insu (vol des mots de passe, accès à distance aux ressources de la machine, destruction de données, etc.). Il n'a pas de facultés autoreproductrices. Voir aussi ver, virus
UCE Unsollicited Commercial E-mail Comme son nom l'indique, du mail non sollicité et commercial. Voir spam. Undisclosed recipient Littéralement : destinataires non révélés Expression placée par certains logiciels de messagerie dans le champ A (ou To:) du courrier électronique, pour signifier que la liste des destinataires est secrète (ou cachée).

URL Uniform Resource Locator Adresse standard de n'importe quel document (page Web, fichier MP3, etc.) sur Internet. En particulier : adresse d'un site Web. L'URL d'azimut.net est ainsi http://www.azimut.net.
Uencode Unix to Unix encoding Comme MIME, UUencode est un codage qui permet d'envoyer des fichiers par le courrier électronique. Il transforme en fait les fichiers binaires (composés de 0 et de 1) en fichiers ASCII (composés de chiffres et de lettres), qui peuvent alors se glisser dans les courriers électroniques. Il faut que le destinataire dispose d'un programme de décodage pour retrouver le fichier au format binaire.
Ver Syn. : worm Programme autoreproducteur. A la différence du virus, il se suffit à lui même : il n'a pas besoin d'un programme hôte pour se reproduire. La méthode la plus courante de propagation des vers est l'envoi de courriers électroniques avec copie du ver en pièce jointe.
Virus Programme dont le but est de se reproduire. Sa technique est de s'accrocher à un programme existant, à la manière d'un parasite. Par abus : virus, ver ou troyen
Webmail Site ou service web permettant d'accéder à son courrier électronique. Worm Voir ver.
ZIP Format d'archivage et de compression de fichiers, très répandu sur PC. NB : ZIP est également le nom d'un lecteur de disquettes de 100 Mo, 250 Mo ou 750 Mo vendu par la société Iomega.