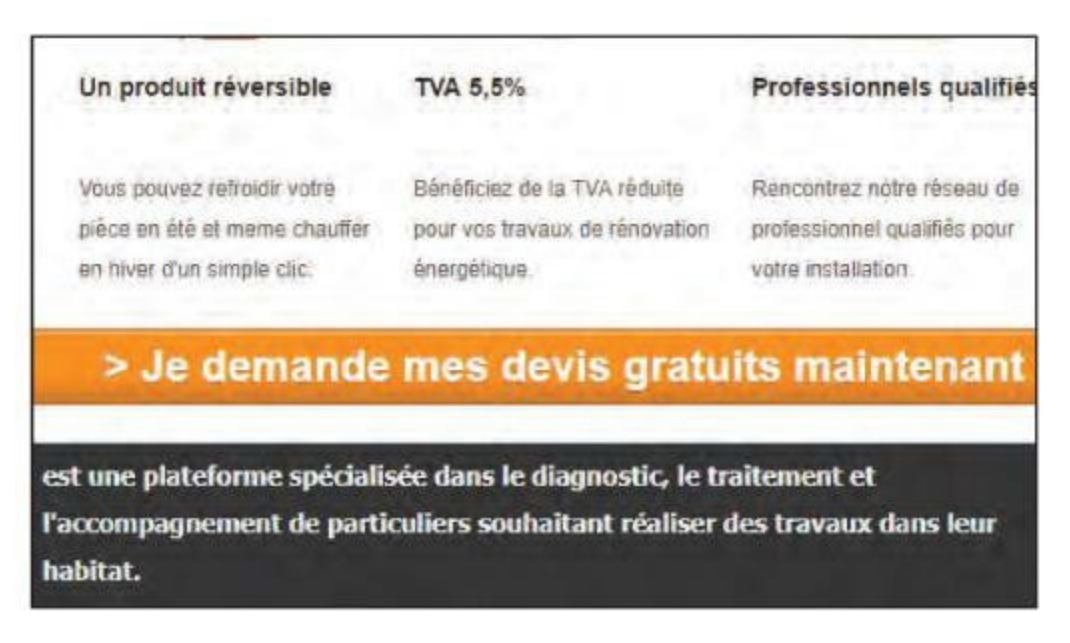
GÉREZ LES INDÉSIRABLES

Les publicités passent de moins en moins les filtres imposés par nos messageries. Du simple désabonnement à la tentative de fraude, voyons comment encore alléger notre boîte de réception.

1 N'HÉSITEZ JAMAIS À VOUS DÉSABONNER

Les messageries s'occupent de filtrer les publicités. Celles qui passent les mailles du filet proposent souvent en bas de page un lien de désabonnement, suivez-le systématiquement. En général, il suffit de cliquer pour être retiré de la liste. Avec un peu de patience, vous serez de moins en moins sollicité.

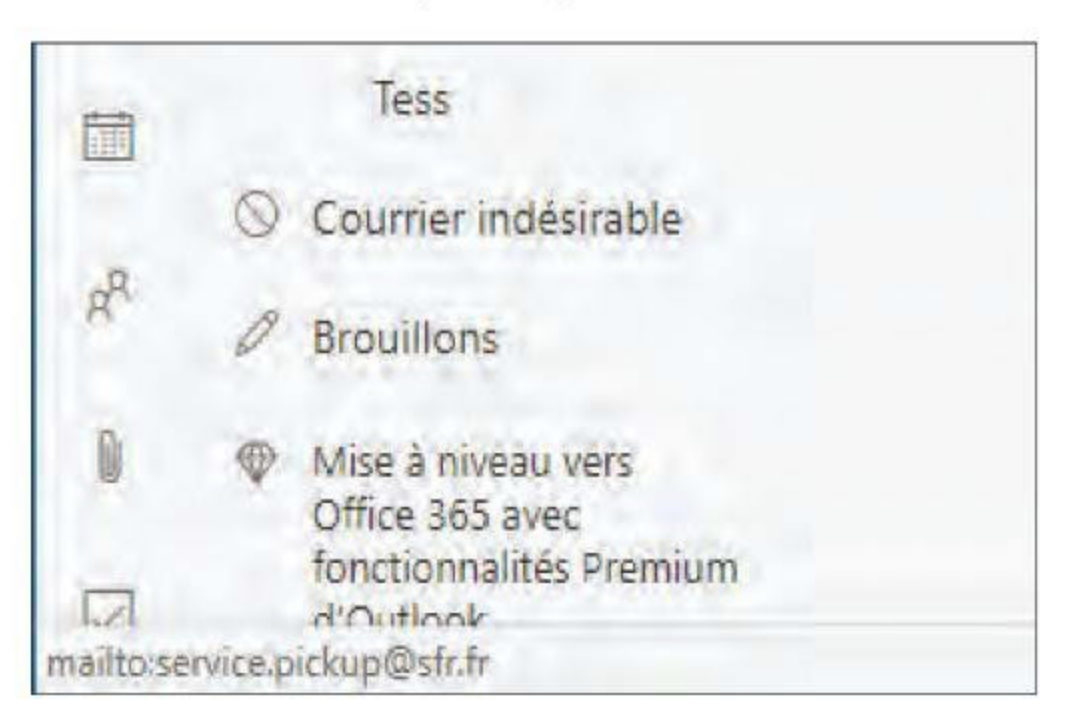


2 REPÉREZ UN SPAM

Beaucoup de spams se repèrent facilement : adresse improbable, fautes d'orthographes. Celui que nous avons pris comme exemple est plus subtil. Il cherche déjà à faire appeler un 08... pour gagner quelques euros. En cas de doute, n'appelez pas un numéro reçu par mail, cherchez le bon numéro sur le Web.

3 CHERCHEZ LA FAILLE PUIS BANNISSEZ

Ce mail présente une adresse Web rassurante : « service@laposte.fr ». Il suffit de passer la souris dessus (sans cliquer) pour que le détail de l'adresse soit donné en bas à gauche de la fenêtre. Elle est différente de celle du contenu dans le mail. Plus de doute, clic droit sur le mail puis *Marquer comme indésirable.*



4 AJOUTEZ UN NOM DE DOMAINE

Les messageries en ligne consacrent une section de leurs paramètres à la chasse aux indésirables. Dans Outlook, vous retrouvez toutes les adresses des expéditeurs bloqués par vos soins. Si vous constatez qu'un nom de domaine est récurrent, ajoutez-le dans la fenêtre Domaines bloqués sans mentionner le @b.

CRÉEZ-VOUS UNE ADRESSE POUBELLE

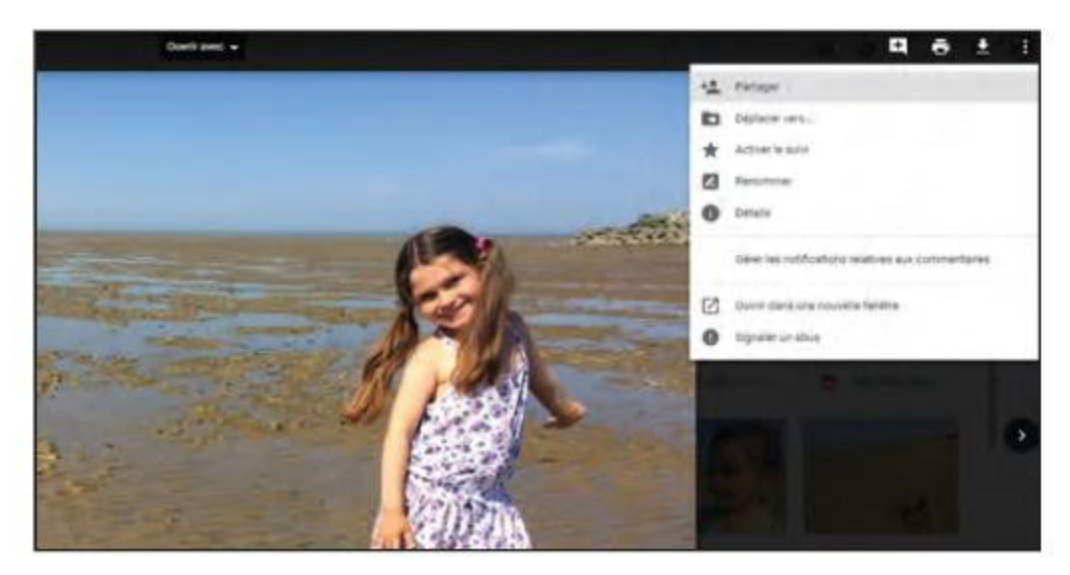
Quelques règles simples, outres celles énoncées précédemment, assurent de réduire le nombre de spams reçus. Lorsque vous vous inscrivez à des cartes de fidélité et autres services d'adhésion, ne donnez votre adresse mail que lorsque c'est indispensable. Cochez les cases *Ne pas communiquer mes données.* Une autre astuce consiste à se faire une adresse à laisser en cas d'inscription obligatoire. Evidemment, cela ne concerne pas les sites marchands, réseaux sociaux et autres services nécessitant votre vraie identité. Un « tapahalsavoir@gmail.com » se chargera de tous les pourriels reçus suite à de la vente de fichiers client. Pensez évidemment à vous y rendre une fois par quinzaine afin de faire le ménage.

LES SERVICES GRATUITS DES MESSAGERIES

Prendre des rendez-vous, stocker des documents, organiser vos tâches, vous aider à travailler... les messageries ne se contentent pas d'être des boîtes de réception, ce sont d'excellents assistants.

1 PROFITEZ DES SERVICES DE CLOUD

Chaque messagerie propose un espace de stockage en ligne. Bon nombre de services sont proposés pour l'exploiter au mieux. Ainsi, vous pouvez par exemple installer l'application liée à une boîte pour stocker les photos de votre smartphone. Mettez aussi en sécurité des documents à garder (factures, papiers administratifs...).

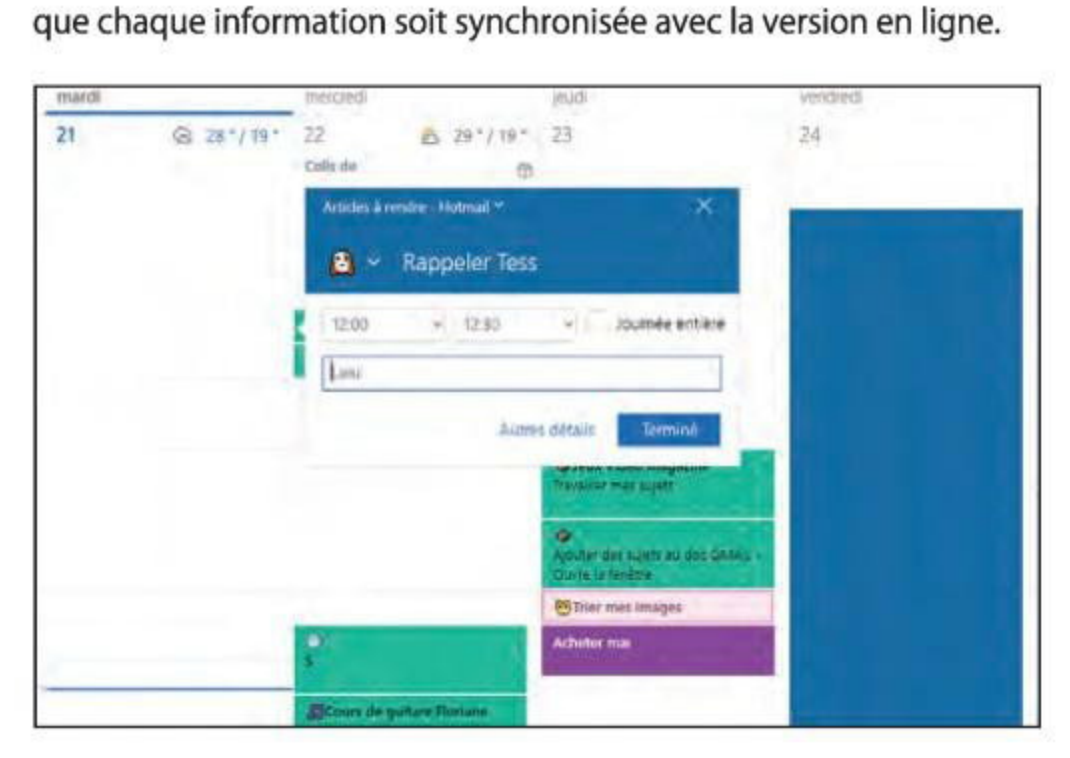


2 LANCEZ DES VISIOCONFÉRENCES

Les mails ne suffisent plus, chaque messagerie propose sa solution d'appels audio et vidéo. Ce sont aussi d'excellents outils de travail grâce auxquels vous pouvez envoyer des documents alors que vous conversez avec un contact. Et évidemment, ces services se retrouvent aussi bien sur ordinateurs que sur mobiles.

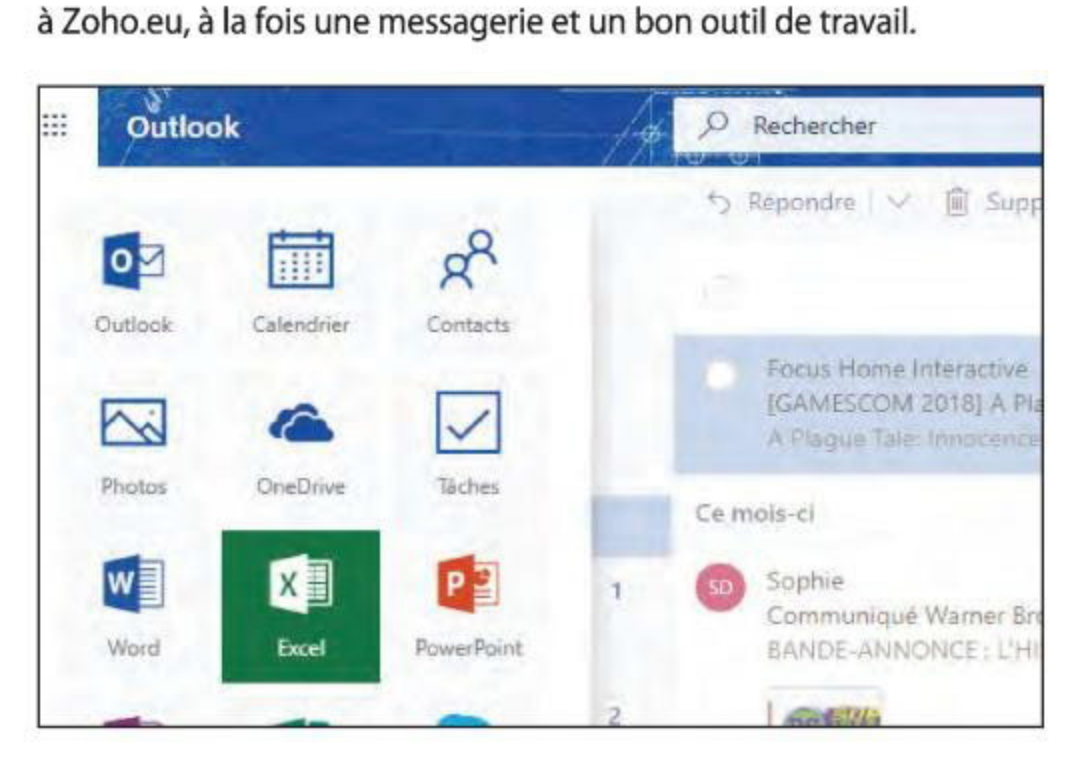
3 PLANIFIEZ VOS TÂCHES ET RENDEZ-VOUS

Chaque messagerie dispose d'un agenda et d'un système de suivi des tâches. Tous ces éléments sont liés à la messagerie pour assurer un suivi. Dans Windows 10, l'application Calendrier, accessible aussi depuis Courrier, permet de gérer son agenda avant que chaque information soit synchronisée avec la version en ligne.



4 TRAVAILLEZ EN TOUTE SIMPLICITÉ

Rien de plus facile aujourd'hui que de travailler en nomade, les messageries de Microsoft et Google proposent leur suite Office. Vous la trouvez dans le Drive de Google en créant un nouveau document ou dans le menu Applications d'Outlook. Pensez aussi à Zoho.eu, à la fois une messagerie et un bon outil de travail.



LES MESSAGERIES DE NOS FAI

Les messageries présentant le maximum de services sont celles de Microsoft et Gmail. Rien de surprenant, elles sont liées à leurs environnements, donc Windows et Android, et font le maximum pour créer un service complet. L'utilisateur est ainsi ravi de travailler, se divertir, communiquer pendant que les deux géants américains font le maximum pour qu'on ne sorte pas de leur pré carré. Nos fournisseurs d'accès à Internet nous octroient aussi une adresse lorsque l'on s'abonne mais les services sont réduits à la portion congrue. Vous pouvez très bien privilégier votre adresse de FAI puis utiliser un service cloud (Dropbox, Mega) et une suite office gratuite (libre office) pour retrouver les mêmes services que Microsoft et Google.

CESSEZ DE CLIQUER SUR DES MESSAGES SUSPECTS !

Des alertes catastrophistes aux mises en garde que l'on vous conseille de faire circuler, les canulars ont encore la vie dure sur Internet et génèrent à tout le moins une diffusion de mails indésirables.

Contrairement au scam et au phishing, les hoax (canulars en anglais) ne vous font pas courir de danger direct. Ils se bornent à leurrer le lecteur en lui faisant avaler une énorme couleuvre. Les sujets traités par les hoax couvrent des thèmes variés et exploitent des ficelles qui paraissent très visibles pour des personnes au fait du sujet mais peuvent pourtant convaincre des personnes crédules ou tout simplement peu informées. Le hoax n'invite qu'à une seule chose : transmettre le message à un maximum de contacts. Il ne présente donc pas de danger direct pour la sécurité. Toutefois, il induit une augmentation inutile du trafic et les listes de diffusion ainsi dévoilées peuvent être mises à profit par les spammeurs. Certains hoax exploitent la peur des virus. Dans un hoax bien connu, apparu il y a dix ans et toujours en circulation, la pièce jointe nommée Ultimas de Atenas, Invitacion ou, plus récemment, Actualisation de Windows Live contient « un virus qui ouvre une torche olympique qui brûle tout le disque dur C de l'ordinateur ». De quoi faire frissonner le non-initié. D'autant que le message précise que « c'est le pire virus annoncé par CNN. Un nouveau virus a été découvert récemment qui a été classé par Microsoft comme le virus le plus destructeur qui ait existé... » Suivent des « explications » pour appuyer les dires : « Il détruit simplement le secteur zéro du disque dur où les informations vitales sont sauvegardées. » D'autres hoax font appel au bon coeur du lecteur. Ici, il faut aider à retrouver une personne disparue. Là, on recherche un donneur de moelle osseuse compatible. Certains de ces hoax peuvent être des canulars dès le départ. D'autres peuvent s'appuyer sur un fait réel mais qui n'est plus d'actualité. Enfin, l'humour noir joue également sur toutes les cordes sensibles. Ainsi par exemple, Le site bonsaikitten.com, aujourd'hui fermé, décrivait la manière d'obtenir des chats « bonsaï » en les élevant dans des bocaux, avec des procédures portant encore plus atteinte à l'animal (anus scellé à la glue, insertion de tubes, etc.). Ce site était en fait un canular monté par d'anciens élèves du très sérieux MIT (Massachusetts Institute of Technology).

UN VIRUS PERSISTANT, UNE PROMESSE DE GAIN SPECTACULAIRE ? RIEN DE TOUT CELA N'EST BIEN SÛR AVÉRÉ !

UNE MAUVAISE BLAGUE TOURNE MAL

Si les hoax sont sans danger direct, il existe tout de même une variante, le viroax (contraction de virus et hoax), beaucoup plus dangereuse. Le message signale qu'il a détecté un virus dans l'ordinateur (on se demande bien comment d'ailleurs !) et se propose de vous aider à l'éradiquer. Suit une liste d'instructions pour effacer un ou plusieurs fichiers, en fait indispensables au bon fonctionnement du système d'exploitation, de l'antivirus, du pare-feu, etc. Faites également attention aux sites d'utilitaires (qui proposent une analyse gratuite de votre système. Non seulement ces derniers se feront fort de vous trouver divers maux mais proposeront une cure payante, en ajoutant diverses barres d'outils et liens publicitaires non désirés : mauvaise blague !

IDENTIFIEZ LES FAUX E-MAILS

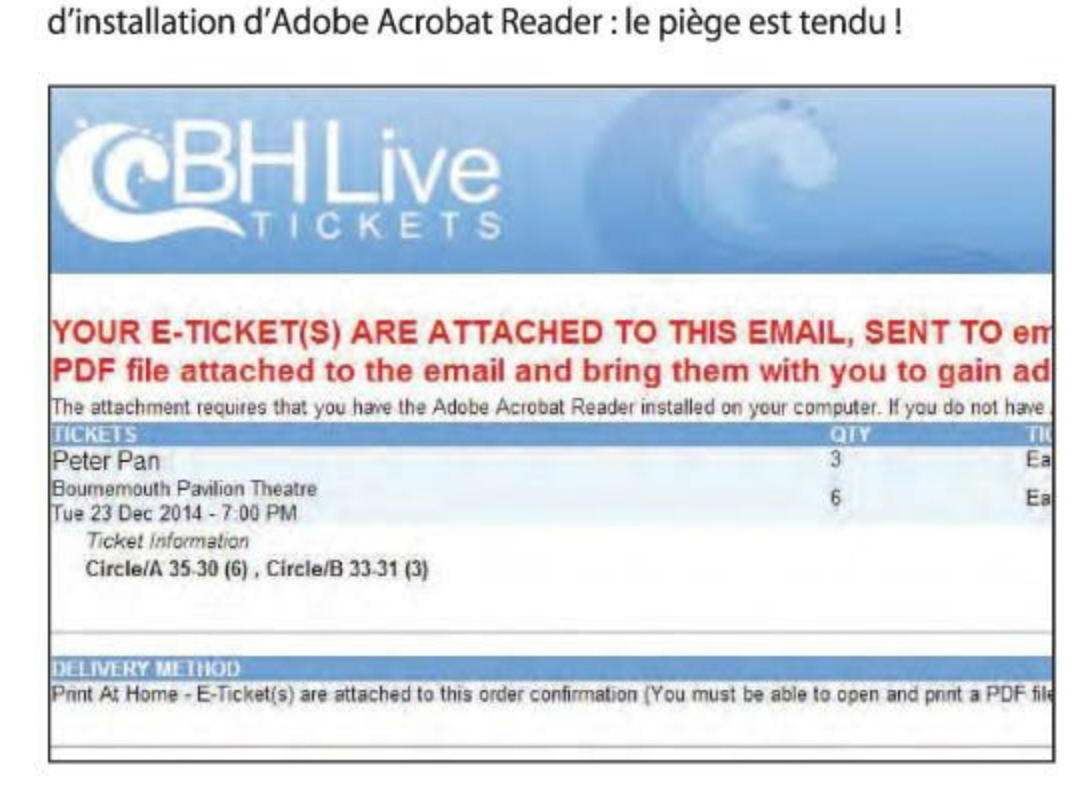
Si vous n'avez pas encore compris que les intitulés des mails sont source de problèmes futurs, suivez cette procédure pas à pas, sélectionnez le courrier et déposez-le directement dans la poubelle.

1 LISEZ LES INTITULÉS

Votre boîte de réception présente chaque jour de nouveaux mails aux intitulés souvent prometteurs. Ne vous précipitez pas d'un clic immédiat et déchiffrez de prime abord l'intitulé du courrier qui vous est adressé. Avec un peu d'attention, il y a de fortes chances que vous déceliez une incitation non désirée.

2 NE CLIQUEZ PAS TROP VITE

Aïe aïe aïe, vous voici récipiendaire d'un ticket de concert alors que vous n'avez rien commandé ! Pour le coup, nous avons cliqué sur ce mail exemple, ce qu'il ne faut justement jamais faire. Derrière cette annonce frauduleuse, une demande d'installation d'Adobe Acrobat Reader : le piège est tendu !



3 NE FAITES PAS RE :

Admettons qu'un de vos proches vous ait écrit, ce qui est, avouons-le, assez fréquent. En réponse, vous pourriez trouver « re : » dans l'intitulé du mail. Mais si vous ne connaissez pas l'expéditeur qui annonce « re » dans l'objet, ne cliquez surtout pas et préférez directement la poubelle de votre messagerie !

4 VOUS N'AVEZ RIEN GAGNÉ

La nouvelle technique du spammeur de base consiste à rédiger un intitulé attractif, du type « votre barbecue en attente de livraison » ou « votre nouveau smartphone disponible ». En consultant vos courriers le matin (pas très réveillé...), vous allez cliquer dessus et simplement perdre du temps !

EXIGEZ LE DÉSABONNEMENT

Les spams commerciaux les plus courants sont émis par des sites qui renvoient ensuite à une loterie mais exigent bien entendu vos coordonnées de messagerie pour valider votre participation à ce jeu de dupe. Si vous avez cliqué sur le message comme nous l'avons volontairement fait, vous trouverez nécessairement une possibilité de désabonnement, car il ne s'agit pas d'une arnaque. Votre demande de désabonnement est généralement prise en compte sous 48 heures. Si cela ne vous suffit pas, sélectionnez le mail concerné et placez-le dans les courriers indésirables.

DES MAILS SOUS FORME D'ATTRAPE-NIGAUD

Une grosse somme d'argent vous est promise et ne demande qu'à être récupérée. Ne rêvez pas: c'est une arnaque qui s'appuie sur la crédulité des victimes et les incite à payer sans fin et sans retour.

Le scam, parfois nommé arnaque nigériane (du fait de l'origine des premières arnaques de ce type) ou fraude 419 (numéro de l'article 4-1-9 du code nigérian visant ce type d'arnaque), est une escroquerie consistant à soutirer de l'argent aux victimes en leur faisant miroiter un gain important. Dans le scam classique, votre interlocuteur dispose d'une grosse somme d'argent. Dans certains cas, il s'agit d'une personne riche qui craint pour sa fortune du fait des désordres politiques dans son pays. Elle cherche à transférer l'argent en France et vous êtes censé recevoir un pourcentage sur ce transfert, ce qui ferait un beau pactole vu l'importance des sommes concernées. Dans d'autres cas, vous êtes l'heureux bénéficiaire d'un héritage (vous ne saviez donc pas que vous aviez un riche oncle inconnu en Afrique noire ?) ou d'un don fait par une personne atteinte d'un cancer en phase terminale et qui vous a choisi (comment vous a-t-elle trouvé et pourquoi vous ?). Dans tous les cas, la victime est incitée à verser toujours plus d'argent pour régler les frais : notaires, pot-de-vin, etc. Les sommes demandées sont rarement importantes à chaque fois mais le total finit par se chiffrer en dizaines de milliers d'euros. Et bien sûr, vous ne percevrez jamais le moindre centime en retour. Vous noterez que les paiements s'effectuent systématiquement via un service de transfert d'argent liquide (Western Union en particulier), les possibilités de recours auprès de cet intermédiaire étant inexistantes.

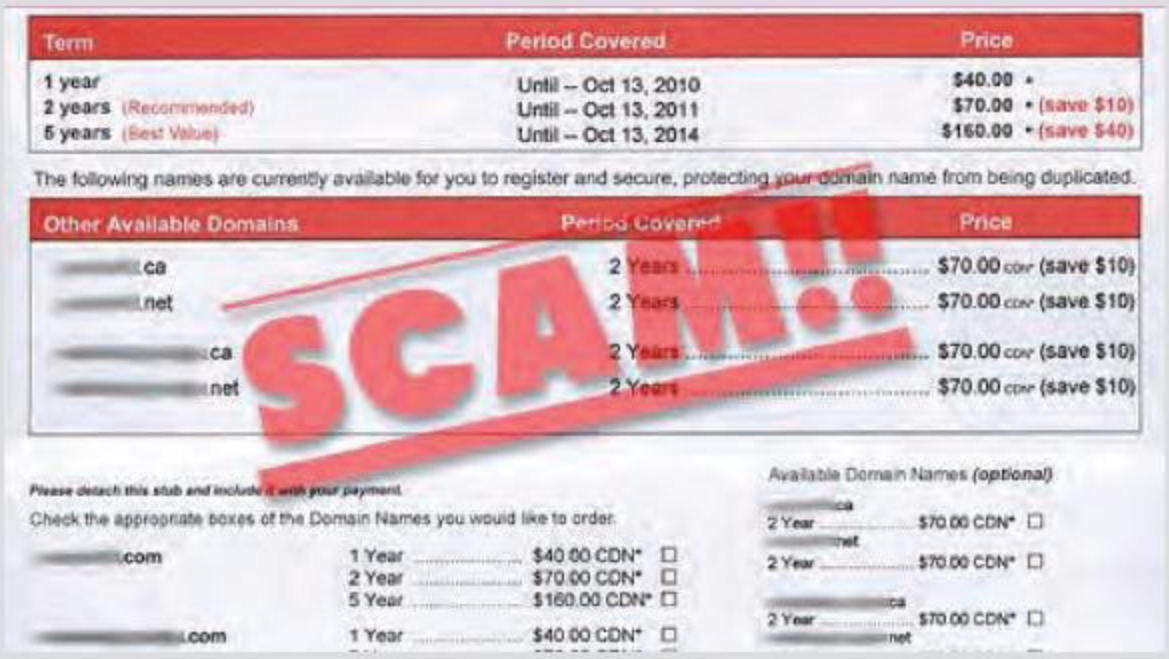
AUCUNE PROMESSE DE GAIN FINANCIER PAR MAIL N'EST À PRENDRE AU SÉRIEUX.

HEUREUX GAGNANT

Dans une variante, vous être l'heureux gagnant d'une « tombola mondiale » destinée à promouvoir un groupe de sociétés ou mise en place par Microsoft (?!). Dans la pièce jointe, vous découvrirez que vous ne gagnez que le cinquième lot (ce qui fait plus vrai) mais qu'il s'agit déjà une somme non négligeable. Un formulaire vous invite à renseigner diverses informations personnelles (pas trop sensibles) et à le renvoyer par mail au notaire mentionné. Là encore, il y aura comme par hasard une succession de frais à régler avant de pouvoir toucher le mirifique pactole. ■

ATTENTION AUX FAUX EMPLOIS

Profitant de la crise ambiante, cette arnaque scandaleuse se décline sous deux formes. Dans la forme classique, la victime reçoit une proposition de travail (fictif bien sûr) et est invitée à payer pour le voyage ou d'autres frais. Dans une variante récente et particulièrement vicieuse, des traducteurs se voient proposer un travail de traduction correctement voire bien payé, avec une avance. Le chèque de l'avance arrive bien, très vite suivi de l'annulation du travail, avec demande de remboursement de l'avance. Si le traducteur s'exécute, il aura perdu la somme correspondante car le chèque initial est en bois, comme ne manquera pas de lui signifier sa banque quelques jours plus tard.



Term	Period Covered	Price
1 year	Until – Oct 13, 2010	$40.00 *
2 years (Recommended)	Until – Oct 13, 2011	$70.00 * (save $10)
5 years (Best Value)	Until – Oct 13, 2014	$160.00 * (save $40)

The following names are currently available for you to register and secure, protecting your domain name from being duplicated.

Other Available Domains	Period Covered	Price
.ca	2 Years	$70.00 CDN* (save $10)
.net	2 Years	$70.00 CDN* (save $10)
.ca	2 Years	$70.00 CDN* (save $10)
.net	2 Years	$70.00 CDN* (save $10)

SCAM!!

Please detach this stub and include it with your payment.

Check the appropriate boxes of the Domain Names you would like to order.

.com	1 Year	$40.00 CDN* ☐
	2 Year	$70.00 CDN* ☐
	5 Year	$160.00 CDN* ☐
.com	1 Year	$40.00 CDN* ☐

Available Domain Names (optional)

.ca	2 Year	$70.00 CDN* ☐
.net	2 Year	$70.00 CDN* ☐
.ca	2 Year	$70.00 CDN* ☐
.net		

NE VOUS FAITES PLUS AVOIR

Les courriers frauduleux les plus dangereux font le plus souvent miroiter des gains exceptionnels, en vous demandant uniquement de servir de relais. Si vous y croyez, le piège se referme assez vite.

1 LISEZ ATTENTIVEMENT LE TEXTE

Bon nombre de scams sont aisément repérables. L'orthographe et la syntaxe souffrent à chaque phrase, les propos sont mystiques (pour les dons) et la proposition trop belle pour être vraie. Certaines fois, vous trouverez même des coordonnées téléphoniques pour vous rassurer.

Subject: I REALLY WISH TO INVEST WITH YOU.
From: George Abed <georgeb@zworg.com>
Reply-To: georgeb@zworg.com
Date: 14.07.2009 18:31
To: [redacted]
content-transfer-encoding: quoted-printable

Dear Sir,

I am George Abed, I know you don't know me in person, of which bad people in this world has made us not to trust the good ones again, but as for me you really need to trust me, my purpose of contacting you is to invest some money with you.

I have the sum of 16,700,000 Euro which i will like to know the kind of investment we can invest the money into,so if you are willing get back to me ,in order for us to discuss on how the fund will be transferred to your account.So feel free to contact me on my direct phone number +22508188984 or you send me an E-Mail: georgeb@zworg.com

Finally, i will be waiting for your response.

2 VISITEZ LE SITE ANTI-ESCROCS

Le site Croque-escrocs.com dresse la liste du top des escrocs scams francophones (à rechercher dans le menu à gauche). Cette liste n'est pas exhaustive mais reste précieuse, car régulièrement mise à jour. Dès que vous doutez d'un mail, c'est une adresse indispensable.

3 RENSEIGNEZ-VOUS SUR INTERNET

Pour les scams « loterie », une rapide recherche sur Internet permettra de dénicher l'imposture, avec de nombreux sites la présentant et les commentaires des victimes sur les forums. Si la loterie est imputée à un éditeur de logiciel ou une grande marque, allez vérifier l'imposture sur son site.

4 FAITES PART DE VOS MALHEURS

Si vous avez été victime d'un scam, consultez le site **www.avenfrance.org**, fenêtre de l'Association des Victimes d'Escroqueries à la Nigériane. Vous y trouverez les recours possibles et de l'aide. N'espérez toutefois pas revoir la couleur de votre argent, car la banque est quasiment dans l'impossibilité de faire opposition.

NE SOYEZ PLUS PIGEONS

Aussi étonnant que cela puisse paraître et en dépit de nos nombreux avertissements répétés, certains d'entre vous tombent encore dans le panneau de ce piège pourtant grossier. Il faut dire que récemment, les intitulés des mails ont changé. En lieu et place de « rendez-moi service ou encore aidez-moi », les nouveaux courriers suspects ont pour objet « félicitations, bravo, vous avez gagné… ». Comment se fait-il que certains internautes croient encore à quelconque gain sorti d'on ne sait où ? Tout simplement parce que l'objet du mail est attractif et déclenche alors un clic réflexe. Et si vous mettiez directement ces intitulés à la poubelle ?