Sécurité internet

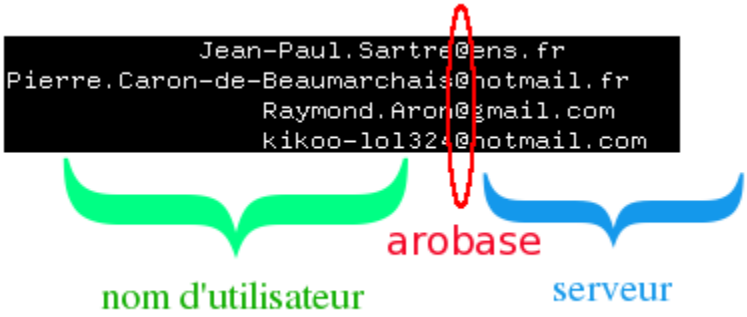
Une adresse électronique est toujours de la forme : utilisateur@machine

Raymond.Aron@gmail.com
Jean-Paul.Sartre@ens.fr
Pierre.Caron-de-Beaumarchais@hotmail.fr
kikoo-lol324@hotmail.com

Le caractère @ s'appelle un *arobase* (ou « a » commercial) et se lit « at ».

Donc, l'adresse president@elisee.gouv se lit « *président at Elisée point gouv* » ;

L'arobase sépare la partie désignant un *humain* (à gauche de l'arobase) de la partie désignant un *ordinateur* (à droite de l'arobase). Tout en minuscule **sans** accent **ni** espace



Dans nos exemples, les **noms d'utilisateurs** sont donc « Raymond.Aron », « Jean-Paul.Sartre », « Pierre.Caron-de-Beaumarchais » et « kikoo-lol324 ». La partie droite de l'adresse, après l'arobase, désigne le **serveur de messagerie**, c'est-à-dire la machine sur laquelle on est inscrit. Dans nos exemples, ce sont « ens.fr », « gmail.com », « hotmail.fr » et « hotmail.com ».

Les attaques d'hameçonnage (Phishing) commencent par un e-mail

Les phishers (ou « hameçonneurs ») vont à la pêche aux informations précieuses.
Par de faux e-mails, ils tentent de dérober des mots de passe ou des données de cartes de crédit ou propager des virus informatiques.

1 "PayPal Inc" <contacto@jondemon.com> - Ce qui est écrit avant l'adresse e-mail ne correspond pas toujours à l'adresse elle-même. Par conséquent, vérifiez soigneusement l'adresse e-mail pour les e-mails suspects.

2 Cher client ... - Ne vous fiez à aucun e-mail ayant une salutation impersonnelle.

3 L'accès à votre compte a été temporairement suspendu - Méfiez-vous des e-mails qui exigent une « action immédiate » ou essaient autrement de vous mettre la pression.

4 Vérifiez le nom, l'adresse et le numéro de facturation - Ne répondez jamais aux demandes par e-mail de mots de passe, de codes de sécurité ou PIN, de numéros de documents officiels, de détails de nom et d'adresse, etc.

5 Clique-moi / Connectez-vous pour commencer - Un lien dans un e-mail ? Déplacez la souris sur le lien et découvrez où il vous mènera.

6 P ayPal - Méfiez-vous des e-mails contenant des fautes d'orthographe et de grammaire.

7 facture.zip - N'ouvrez que les pièces jointes des expéditeurs en qui vous avez confiance et que vous attendez. Même les pièces jointes d'amis ou de membres de la famille peuvent contenir des logiciels malveillants - leurs comptes peuvent être piratés ou infectés.

Comment reconnaître un mail de phishing ou d'hameçonnage ? - Assistance aux victimes de cybermalveillance

(Cliquez sur le lien en bleu pour accéder au site)

1. Une notification de la messagerie ou de l'antivirus

Votre messagerie ou votre antivirus peuvent vous signaler la réception d'un mail frauduleux.

2. Un email d'un service ou d'une société dont vous n'êtes pas client

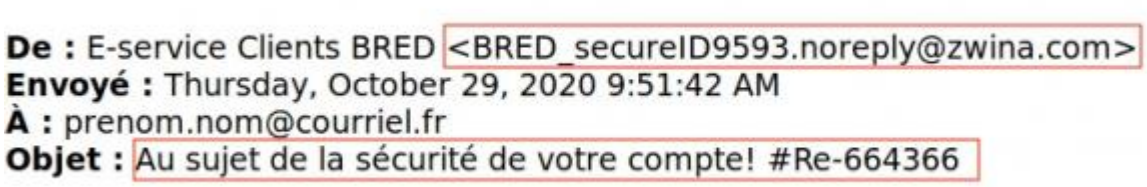
Si vous recevez un email d'un service ou d'une société dont vous n'êtes pas client, méfiez-vous.

3. Mail phishing : un nom d'expéditeur inhabituel

La réception d'un message inattendu d'une adresse email inhabituelle, que vous ne connaissez pas ou qui ne fait pas partie de vos contacts, doit éveiller votre attention

4. Une adresse d'expédition fantaisiste

. **Pour vérifier qu'il s'agit bien d'un message officiel, pensez à vérifier l'adresse email de l'expéditeur.** Si cette dernière ne comporte pas le nom de l'entité, qu'elle présente des fautes d'orthographe ou que le nom vous paraît suspect, n'ouvrez pas le message. Il s'agit sûrement d'un mail frauduleux.



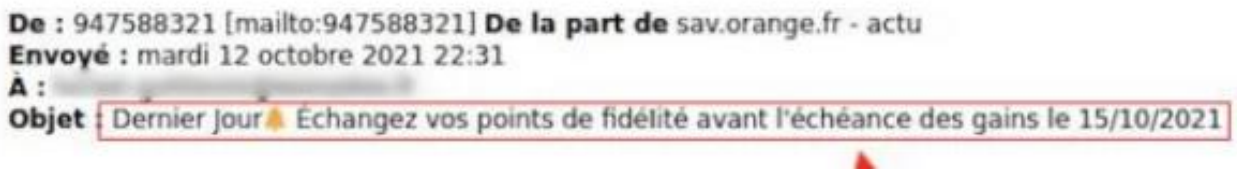
Mail de phishing

avec une adresse mail suspecte et un objet de mail alarmiste.

Message de phishing aux couleurs de l'Assurance Maladie avec une adresse mail fantaisiste.

5. Un objet d'email trop alléchant ou alarmiste

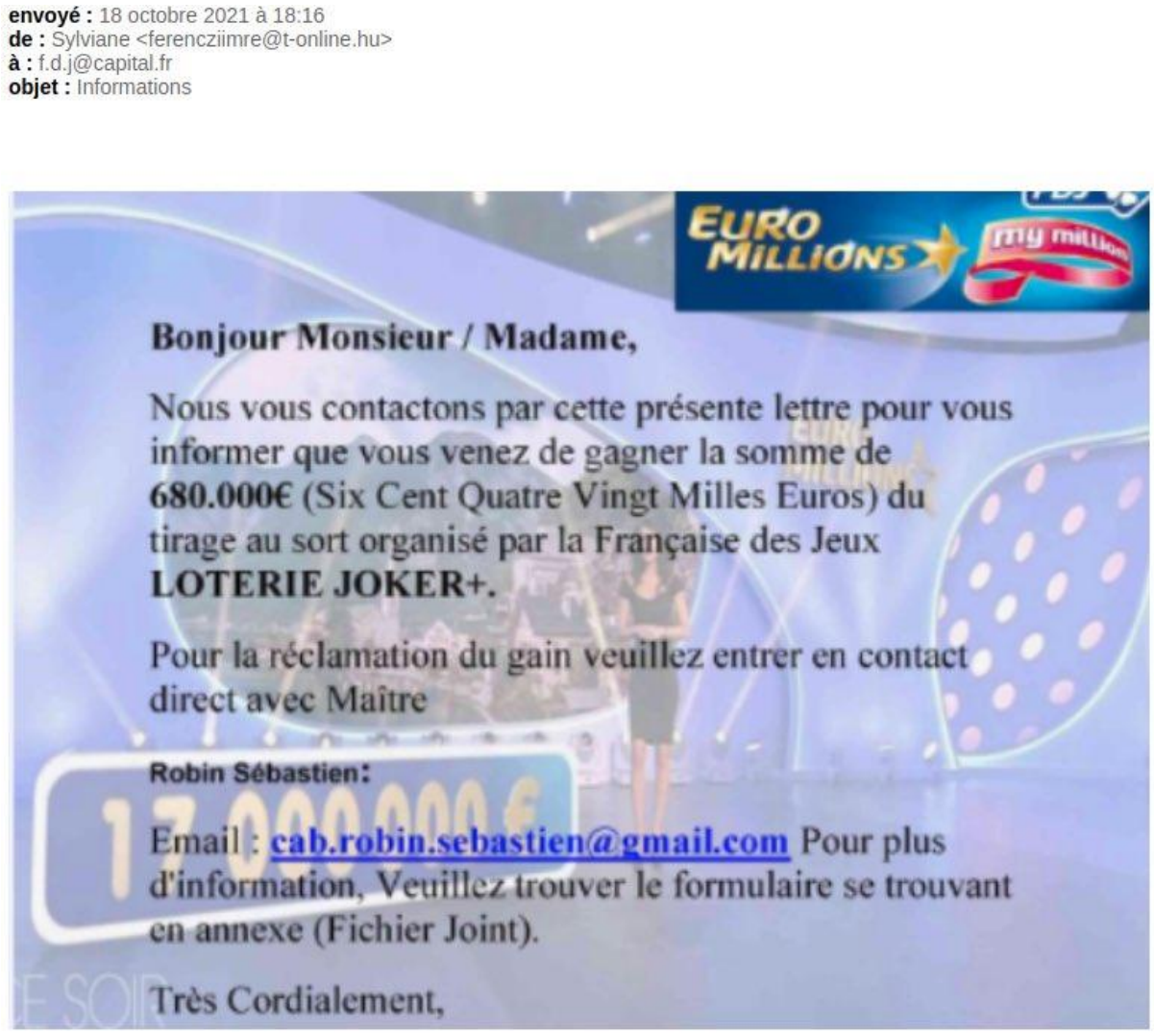
L'objet d'un mail de phishing est généralement sommaire et cherche à inciter la victime à ouvrir le message. **Un intitulé aguicheur ou inquiétant** – comme « remboursement » ou « alerte de sécurité » – qui transmet un sentiment d'urgence inhabituel.



Exemple d'un mail de phishing aux couleurs d'Orange avec un objet de mail aguicheur et alarmiste.

6. Une apparence suspecte

Images et logos de mauvaise qualité, flous, déformés, pixelisés ou pris de loin, peuvent être le signe qu'il s'agit de captures d'écran ou d'éléments volés sur des sites officiels.



Mail frauduleux aux couleurs de la Française des jeux à l'apparence suspecte.

7. Une absence de personnalisation

Généralement, les emails officiels qui vous sont adressés mentionnent votre nom, or **l'hameçonnage « bon marché » consiste à envoyer à échelle industrielle le même mail de phishing de manière dépersonnalisée**.

8. Une demande inhabituelle

Connaître l'adresse email de l'expéditeur n'est pas un critère de confiance absolu : le cybercriminel peut avoir usurpé l'adresse de messagerie d'un proche ou d'un service connu. Soyez vigilant aux éléments suspects, notamment si le message contient un lien cliquable, une pièce jointe, ou vous demande des informations.

9. Une demande d'informations confidentielles

En règle générale, les demandes d'informations personnelles – identifiants de connexion, informations bancaires… – ne se font jamais par email. Aucune entité légitime, gouvernementale, professionnelle ou autre n'est en droit de vous demander votre code de carte bancaire ou vos codes d'accès personnels par message. **Ne communiquez rien de confidentiel par écrit**, même s'il s'agit d'un expéditeur qui prétend faire partie de votre entourage.


Envoyé: vendredi 15 Octobre 2021 11:07
De : "Relation Clientèle Floa-Bank"
A :
Objet : Authentification-Mobile

FLOA bank

Bonjour,

En accord de la Directive européenne,

La double authentification devient une obligation.

Confirmer votre mobile ici

Nous vous remercions de votre confiance.

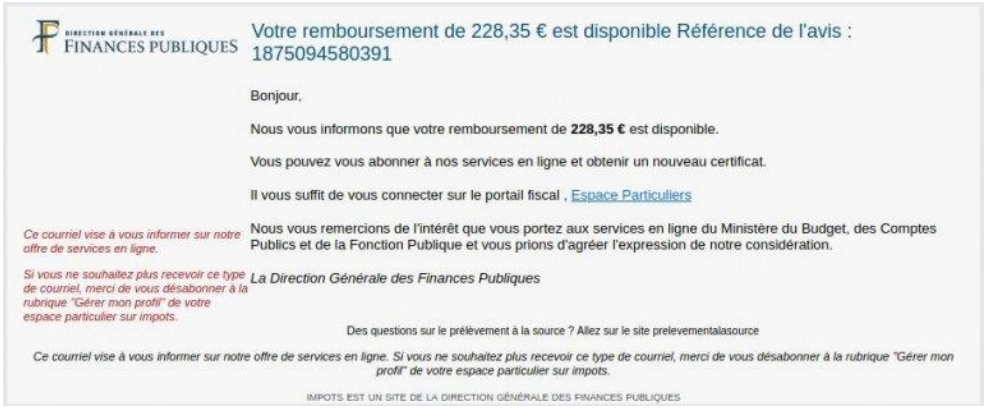
Cordialement,
Votre Conseiller FLOATBANK.

1) Sous réserve d'un fonctionnement normal de votre compte et du solde disponible lorsdu traitement de votre demande.FLOABANK
, Société Anonyme au capital de 41 228 000 euros – Bâtiment G7, 71 Rue Lucien Faure, 33300 Bordeaux, RCS Bordeaux 434 130 423, ORIAS n°07 028 160, Entreprise soumise au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) 4 Place de Budapest, CS 92459, 75430 Paris Cedex 09.
Ce message et toutes les pièces jointes sont confidentiels et établis à l'intention exclusive de son ou ses destinataires. Si vous avez reçu ce message par erreur, merci d'en avertir immédiatement l'émetteur et de détruire le message. Toute modification, édition, utilisation ou diffusion non autorisée est interdite. L'émetteur décline toute responsabilité au titre de ce message s'il a été modifié, déformé, falsifié, infecté par un virus ou encore édité ou diffusé sans autorisation.

Exemple de faux mail demandant des informations personnelles (un numéro de téléphone mobile).

10. Un message aguicheur ou inquiétant

Un mail de phishing fait souvent part d'une offre, d'un remboursement ou d'un gain inespéré. Un mail frauduleux peut également faire état d'un besoin urgent ou d'une menace imminente qui requiert une action immédiate, comme la fermeture de votre compte si vous n'agissez pas tout de suite.


DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Votre remboursement de 228,35 € est disponible Référence de l'avis : 1875094580391

Bonjour,

Nous vous informons que votre remboursement de **228,35 €** est disponible.

Vous pouvez vous abonner à nos services en ligne et obtenir un nouveau certificat.

Il vous suffit de vous connecter sur le portail fiscal , Espace Particuliers

Nous vous remercions de l'intérêt que vous portez aux services en ligne du Ministère du Budget, des Comptes Publics et de la Fonction Publique et vous prions d'agréer l'expression de notre considération.

La Direction Générale des Finances Publiques

Ce courriel vise à vous informer sur notre offre de services en ligne.

Si vous ne souhaitez plus recevoir ce type de courriel, merci de vous désabonner à la rubrique "Gérer mon profil" de votre espace particulier sur impots.

Des questions sur le prélèvement à la source ? Allez sur le site prelevementalasource

Ce courriel vise à vous informer sur notre offre de services en ligne. Si vous ne souhaitez plus recevoir ce type de courriel, merci de vous désabonner à la rubrique "Gérer mon profil" de votre espace particulier sur impots.

IMPOTS EST UN SITE DE LA DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

11. Mail phishing : des fautes de français surprenantes

Soyez vigilant à la qualité du texte de l'email. L'hameçonnage par mail comporte souvent des fautes de frappe, d'orthographe ou de grammaire. Des erreurs de formulation, de mauvaise traduction ou une syntaxe inhabituelle dans des communications officielles doivent également vous alerter.

12. Une incitation à cliquer sur un lien ou une pièce-jointe

Un mail de phishing cherche généralement à pousser la victime à cliquer sur un lien. Avant de cliquer, pensez à vérifier l'adresse des sites web mentionnés. Pour cela, positionnez le curseur de votre souris sur le lien proposé **sans cliquer** afin d'afficher le lien complet et l'adresse où il mène réellement. Pour vérifier que l'adresse correspond exactement à la page de connexion officielle, rendez-vous directement sur le site de l'organisme en question en saisissant manuellement son adresse dans votre navigateur.

Un mail de phishing peut également vous inciter à ouvrir ou télécharger une pièce jointe (une image, un fichier audio ou vidéo, un document PDF, une pièce jointe au format HTML…). Évitez ainsi de cliquer sur des pièces jointes que vous n'attendiez pas, envoyées par des expéditeurs inconnus ou douteux. Une fois ouverte, la pièce jointe peut vous rediriger vers un site frauduleux vous réclamant des informations confidentielles, voire installer un virus sur votre ordinateur ou votre téléphone.

Exemples de mails qui doivent vous alerter

- **Demande de mise à jour ou de confirmation de données personnelles** – identifiants, mots de passe, coordonnées bancaires… – par un prétendu organisme public ou commercial de confiance, sous peine de sanction.
- **Défaut de paiement ou problème de facturation** : un faux mail vous informe qu'un bien ne peut être expédié en raison d'un problème de facturation ou que vous devez régler un impayé.
- **Demande d'informations inattendue** pour un remboursement, une annulation de commande, une livraison, etc.
- **Demande d'informations contre l'envoi d'un cadeau** ou pour participer à un jeu-concours avec un gain attrayant, ou encore pour récupérer le gain d'une loterie.
- **Demande de règlement** pour éviter la fermeture d'un accès.
- **Appel aux dons frauduleux**.
- **Appel à l'aide** : le cybercriminel se fait passer pour un proche, expliquant qu'il se trouve dans une situation désastreuse qui requiert votre aide financière.
- **Les chaînes d'emails** type porte-bonheur, pyramide financière, appel à solidarité ou alerte virale, peuvent dissimuler une tentative de phishing.

Sources : cyber surveillance.gouv.fr

Pour vérifier vos connaissances Quiz SG : reconnaître les messages frauduleux - SG

Quiz : Testez vos connaissances en matière de cybersécurité - rtbf.be