Comment vérifier la fiabilité d'un e-mail

Dernière modification le 06 avril 2022

Résumé

Ce tutoriel explique les bons réflexes à adopter pour identifier et traiter les e-mails suspects. Les principaux risques auxquels nous nous exposons à la réception d'un e-mail sont : le phishing (ou hameçonnage), la circulation de virus, les arnaques, les fausses nouvelles (Fake news)...

Prérequis

- Disposer d'une adresse e-mail
- Savoir accéder à sa messagerie Savoir ouvrir un e-mail

Les précautions élémentaires

Pour toute réception de mail douteux, évitez ces actions :

- ~~C~~liquer sur un lien hypertexte Répondre au mail
- Cliquez sur un lien qui semble connu, saisissez directement l'adresse URL (ou lien) sur votre navigateur.
- ~~A~~fficher les images qui ne l'ont pas été automatiquement

- Ouvrir une pièce jointe, si vous avez un doute sur l'émetteur ou le message

Consulter les e-mails placés dans les dossiers « spam » ou « indésirable ». Sauf si vous êtes certain de leur sécurité. Supprimer les sans attendre afin d'éviter de les ouvrir par erreur quelque temps plus tard.

Astuces :

Si vous hésitez à supprimer un mail, **cliquez** sur l'adresse de l'émetteur afin de la vérifier.N'hésitez pas à signaler les spams et autres faux messages sur les sites officiels

Signal Spam ou Phishing Initiative.

Respectez la règle du R.L.V : Recul, Lecture et Vigilance.

Que faire en cas d'e-mail suspect ?

Émetteur suspect

Si vous recevez un mail d'un organisme public ou privé sur lequel vous avez créé un espace (par exemple impots.gouv.fr), **ne cliquez pas sur les liens proposés**, **connectez-vous** directement sur votre compte pour vérifier l'information. **Placez** (sans cliquer) le curseur de la souris sur le texte du lien, l'adresse du site de destination s'affiche.Les grandes structures connues (Sécurité sociale, Impôts, banques...) ont un nom de domaine bien identifié. S'il semble inconnu ou suspect, méfiez-vous ! Ne cliquez pas sur les liens., passez la souris dessus pour afficher les informations complémentaires.Dans cet exemple, il n'y a aucun doute : le domaine ameli.fr est bien celui de l'Assurance Maladie :

Prétexte curieux

L'objet du mail frauduleux évoque souvent un sujet peu ordinaire. En voici quelques exemples :

Un prétendu pirate aurait trouvé des vulnérabilités sur votre site Internet et demande une rançon pour ne pas les exploiter

Un ami aurait besoin d'aide, mais refuse d'être appelé par téléphone

Un organisme important (votre banque, EDF, etc.) aurait perdu votre identifiant et votre mot de passe à la suite d'un incident technique

Une entreprise vous annonce que vous avez oublié de lui régler une facture ou vous accorde le remboursement d'un trop perçu

Des félicitations pour avoir gagné un lot important lors d'un tirage au sort dont vous n'avez jamais entendu parler

Une proposition d'investir dans une affaire très rentable

Une demande de don pour une association caritative avec laquelle vous n'avez aucune relation

Information merveilleuse ou farfelue

Pour les mails informant d'une fausse nouvelle extraordinaire comme la découverte d'un nouveau vaccin, la vente d'un objet de luxe à prix dérisoire, la découverte d'une île inexplorée etc. Ne jamais les diffuser avant d'avoir contrôlé leur véracité .

Vérifiez les fausses informations sur le site de Hoaxbuster.

Lexique

Phishing (hameçonnage) : Technique de fraude par courriel, basée sur l'usurpation d'identité de banques ou d'entreprises commerciales, afin d'obtenir de particuliers des renseignements confidentiels (numéros de cartes de crédit, par exemple).(source larousse.fr)

Fake news (fausse information) : sur Internet, faux article de presse destiné à abuser la confiance du lecteur ; par extension, courant, information fabriquée, biaisée ou tronquée diffusée par un média ou un réseau social dans le but de tromper l'opinion publique. (source larousse.fr)

Pour aller plus loin - liens utiles

- Informations sur le site de la CNIL
- Signal Spam

Licence