Comment détecter un mail malveillant ?

publié le 17/07/2015 - mis à jour le 18/07/2015

Descriptif :

Fiche pratique CNIL

Fiche pratique CNIL

Certaines personnes malintentionnées tentent de mettre la main sur vos données personnelles via des techniques d'hameçonnage (phishing) ou d'escroquerie de type fraude 419 (scam) ! Ces techniques d'attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un mail est légitime ou non.

Comment repérer une arnaque par mail ?

Est-ce que le mail vous est réellement destiné ?

1. Généralement, les mails malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.
2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un mail malveillant.

- Attention aux expéditeurs inconnus : soyez particulièrement vigilants sur les mails provenant d'une adresse que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
- Soyez attentif au niveau de langage du mail : même si cela s'avère de moins en moins vrai, certains mails malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration …).
- Vérifiez les liens dans le mail : avant de cliquer sur les éventuels liens, laissez votre souris dessus*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouvv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr .

* A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.

- Méfiez vous des demandes étranges : posez-vous la question de la légitimité des demandes éventuelles exprimées dans le mail que vous lisez. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.
- L'adresse mail source n'est pas un critère fiable : une adresse mail provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un mail.

Comment réagir ?

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime :

- N'ouvrez surtout pas les pièces jointes et ne répondez-pas ;
- Signalez-le auprès de la plateforme **signal-spam** ;

- Déplacez ce mail dans la corbeille puis videz la corbeille ;
- S'il s'agit de votre compte mail professionnel : transférer-le au SII et RSSI de votre entreprise pour vérification. Attendez la réponse avant de supprimer le mail.

Comment s'en prémunir ?

- Utilisez un logiciel de filtre anti-pourriel ou activer l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs.
- Installez un anti-virus et mettez-le à jour.
- Désactivez le volet de prévisualisation des messages.
- Lisez vos messages en mode de texte brut.

Si vous êtes victime d'une escroquerie ?

Signalez les escroqueries auprès du site **www.internet-signalement.gouv.fr**, la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements.