LUTTER CONTRE LE PHISHING

OU HAMEÇONNAGE

QUI SONT LES HAMEÇONNEURS ?

Une minorité dont les connaissances et compétences élevées en informatique leur permettent de réaliser des méfaits pointus et ciblés. Leur objectif est d'engranger, en une seule fois, un gain financier considérable.

Et les autres – la plus grande majorité – qui utilisent des solutions "clé en main" : comme le rappelle l'ANSSI dans une communication du 31 janvier 2019, "cette profusion d'attaques est facilitée par la vente sur Internet de rançongiciels prêts-à-l 'emploi (raas : ransomware-as-a-service), comme gandcrab, ryuk, samsam, dharma...

COMMENT REPÉRER UN MAIL DE PHISHING ?

Si les emails de phishing sont conçus pour être quasi-similaires aux mails dont ils ont usurpé l'identité, il est parfois possible de repérer les signaux d'une tentative de phishing. Bien que l'hameçonnage se présente sous diverses formes, on retrouve en effet souvent des indicateurs similaires

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, même si celle-ci est d'apparence légitime. Si l'adresse email de l'expéditeur vous paraît suspecte, posez-vous les questions suivantes : connaissez-vous l'expéditeur ? Est-il possible que ce dernier vous adresse un message ? Est-ce que le contenu du message vous est réellement destiné ? Est-ce que le sujet abordé vous parle ? S'il s'agit d'un mail de phishing envoyé à échelle industrielle, il sera en effet très peu personnalisé.

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

Les cybercriminels envoient parfois leur mail de phishing au hasard. Si vous recevez un email d'un service ou d'une société dont vous n'êtes pas client, méfiez-vous.

Une notification de la messagerie ou de l'antivirus

Votre antivirus peut vous signaler la réception d'un mail frauduleux. N'ignorez pas son avertissement et assurez-vous régulièrement que votre antivirus est activé et à jour.

Une adresse d'expédition fantaisiste

La plupart des phishing par email utilisent des adresses de messagerie qui ne ressemblent pas à des adresses officielles. Pour vérifier qu'il s'agit bien d'un message officiel, pensez à vérifier l'adresse email de l'expéditeur. Si cette dernière 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.

A FAIRE ET À NE PAS FAIRE !

- **Vous recevez des alertes de votre banque ou autre société vous informant que votre compte est sur le point d'être fermé ?**

  Ne vous fiez jamais à ce type d'alerte

- **Si vous recevez un e-mail vous demandant tout type d'informations de compte**

  Supprimez-le immédiatement, puis appelez l'entreprise concernée pour confirmer l'absence de problème concernant votre compte.

- **Si un courriel vous semble douteux**

  Ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient !

- **Vous réglez un achat en ligne et que vous devez donc fournir des informations relatives à votre carte bancaire**

  Vérifiez que vous êtes sur un site web sécurisé dont l'adresse commence par « https »

- **On vous demande des informations confidentielles par mail ?**

  Aucun site web fiable ne vous le demandera !

SE PROTÉGER DE L'HAMEÇONNAGE, C'EST ÊTRE RESPONSABLE

De manière générale :

- Ne **partagez jamais** vos informations, soyez prudent lorsque vous partagez des informations personnelles ou professionnelles ;
- Observez bien l'URL du lien, toute faute d'orthographe ou irrégularité doit attirer votre attention ;
- Vérifiez que le site est sécurisé : un cadenas doit être présent dans l'URL et l'adresse du site doit commencer par HTTPS (et non HTTP)

Concernant votre boite mail :

Certes, il arrive que le manque de temps et la fatigue engendrent une baisse de vigilance. Toutefois, prenez le temps de vous poser les bonnes questions.

- Est-ce que cet e-mail m'est réellement destiné ?
- Ce message évoque un dossier, une facture, un thème qui ne me parle pas ?
- Est-ce que je connais cet expéditeur ? Son contenu est inquiétant, déconcertant, inattendu ?
- Pourquoi cet expéditeur me somme-t-il de répondre dans de si brefs délais ?

En cas de doute, ne cliquez pas sur "répondre" ou "transférer".

De plus, ne cliquez jamais sur les liens ou pièces jointes des emails. Ils dirigent souvent vers une fausse page qui ressemble au site d'origine ou téléchargement d'un logiciel malveillant.

Sources :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage

https://www.kaspersky.fr/resource-center/preemptive-safety/phishing-prevention-tips