SE PROTEGER CONTRE LE PHISHING

C'EST QUOI LE PHISHING ? (PRONONCEZ « FISHING »)

Il s'agit d'une technique d'escroquerie sur internet, aussi appelée « hameçonnage », visant à récupérer

- vos données personnelles : nom, prénom, date de naissance, téléphone, adresse postale,…
- vos coordonnées bancaires, numéro de carte de crédit
- vos comptes de connexion : compte Windows, sites bancaires et marchands, réseaux sociaux,…

Les pirates informatiques utilisent ensuite ces données pour usurper votre identité et ainsi mener des opérations frauduleuses : achats débités sur votre compte ou facturés à votre société, falsification de documents, vol de données, envoi de message en votre nom,…

La technique utilisée

Pour obtenir ces informations, les pirates envoient un mail frauduleux qui semble provenir d'un service ou organisme de confiance (service comptabilité ou informatique de votre entreprise, votre banque, votre fournisseur internet,…) vous invitant dans un délai assez court :

- à répondre directement au mail
- à cliquer sur un lien
- ou à ouvrir une pièce jointe

COMMENT SE PROTEGER ?

Sachez identifier une tentative de phishing

- L'adresse mail de l'expéditeur comporte des anomalies
- Le texte du message contient des fautes d'orthographes et des tournures de phrases inhabituelles
- Le prétexte mis en avant fait ressortir un besoin d'urgence vous incitant à
    - ouvrir une pièce jointe ou à cliquer sur un lien
    - fournir des informations confidentielles (ex : mots de passe, code PIN, coordonnées bancaires, etc…).

Si vous avez un doute

- Téléphonez directement à l'organisme ou à la société en question pour vérifier l'authenticité du message
- Enregistrez la pièce jointe sur votre disque puis scannez le fichier avec l'antivirus
- Faites analyser le mail par votre correspondant informatique ou support local

Si vous avez reçu un mail suspect

- Ne répondez pas au mail
- Ne cliquez sur aucun lien contenu dans le mail
- N'ouvrez pas les pièces jointes
- Prévenez la personne ou l'organisme dont l'identité a été usurpée
- Signalez le mail frauduleux à votre correspondant informatique ou support local
- Détruisez le mail

Si vous avez déjà répondu au mail frauduleux

- Prévenez la personne ou l'organisme dont l'identité a été usurpée
- Modifiez les mots de passe transmis par inadvertance
- Si votre poste a un comportement anormal, faites-le contrôler par le support informatique
- Consultez vos relevés de compte bancaire et assurez-vous qu'aucun montant n'a été prélevé

POUR ALLER PLUS LOIN

ILLUSTRATION D'UN MAIL FRAUDULEUX

COMMENT IDENTIFIER UNE TENTATIVE DE PHISHING ?

EXEMPLE EN VIDEO :

HTTPS://WWW.HACK-ACADEMY.FR/CANDIDATS/WILLY

COMMENT IDENTIFIER UNE TENTATIVE DE PHISHING ?

ILLUSTRATION D'UN MAIL FRAUDULEUX

SOYEZ ATTENTIF A TOUT INDICE METTANT EN DOUTE L'ORIGINE REELLE DU MAIL

L'**adresse mail de l'expéditeur** s'apparente au nom de l'organisme ou de la société mais **comporte souvent des anomalies** (incohérence de l'adresse mail et le nom de l'organisme)

Passez votre curseur de souris sur le nom de la personne qui vous a envoyé le mail.

*En faisant cela, vous serez en mesure de dire si le mail provient d'un domaine reconnaissable qui est lié au nom réel de l'expéditeur. Exemple : **@freemobile.fr.bouygues-construction.com***

Les techniques se sont nettement améliorées. Les textes sont cohérents, le logo et la signature sont la réplique exacte du site d'une administration d'une société que vous connaissez bien

Toutefois, méfiez-vous des mails suspects contenant des fautes d'orthographe grossières, des fautes de grammaire, des tournures de phrase inhabituelles, des caractères issus d'alphabets étrangers.

Les **prétextes** souvent mis en avant pour vous inciter à répondre sont :

- une mise à jour de vos données personnelles
- la désactivation imminente de votre compte (par exemple : coupure de fourniture d'électricité)
- un remboursement ou une remise (par exemple : une réduction d'impôt)
- la livraison d'un colis

Si un email semble trop beau pour être vrai, il s'agit probablement d'une arnaque

En général, le **mail peut contenir**

- soit **une pièce jointe** (formulaire à remplir, programme à exécuter, etc…) contenant un logiciel malveillant ou un virus

- soit **un lien** qui renvoie vers un site Internet frauduleux ressemblant fortement au site officiel et vous demandant de saisir des informations confidentielles (n° carte bancaire, code d'accès,…)

Passez votre curseur de souris sur le lien fourni dans le mail.

En faisant cela, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message