SYNDESIN
ACCOMPAGNEMENT NUMERIQUE

Mes fiches mémos

INTRODUCTION

L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer un internaute pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. Cette arnaque peut être réalisée via différents canaux de communication : courriels (emails), réseaux sociaux, messagerie instantanée, SMS…

Pour arriver à se prémunir de ce type d'arnaques par message électronique et savoir y faire face en cas de besoin, il est important de bien comprendre leur fonctionnement.

Tendant à se développer et à se diversifier, les attaques par hameçonnage ciblent aussi bien les particuliers que les professionnels : en 2019, l'hameçonnage représente en effet la première menace pour les entreprises, avec 23% des recherches d'assistance sur la plateforme www.cybermalveillance.gouv.fr, et la troisième menace pour les particuliers avec 16%.

Leur caractère de plus en plus massif réside certainement dans la facilité qu'ont aujourd'hui les cybercriminels à se procurer sur les marchés noirs, des bases d'adresses de messagerie conséquentes issues de fuites de données qui ont frappé certaines grandes plateformes Internet ces dernières années.

Les cybercriminels jouent ensuite sur un certain nombre de paramètres pour piéger leurs victimes, tels que la peur, l'appât du gain ou la crédulité.

SYNDESIN vous délivre quelques **recommandations pour vous permettre d'identifier et déjouer ces arnaques par message électronique.**

QU'EST-CE QU'UNE ARNAQUE PAR HAMEÇONNAGE VIA MESSAGE ELECTRONIQUE ?

L'hameçonnage (phishing en anglais) désigne une technique frauduleuse, qui peut relever en fonction du cas d'espèce, de la tentative d'escroquerie au travers de l'envoi d'un message électronique.

L'objectif du cybercriminel ? **Récupérer des données personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux.**

Les informations demandées concernent généralement :

- Des données personnelles : nom, prénom, adresse postale ou de messagerie, numéro de téléphone…
- Des identifiants de connexion : nom d'utilisateur, mot de passe…
- Des informations bancaires : RIB, numéro de carte bancaire…

Autrefois facilement identifiables, ces arnaques par message électronique apparaissent de mieux en mieux réalisées et même les internautes les plus avertis peuvent parfois s'y méprendre.

Le procédé est le suivant :

1. Vous recevez un message électronique frauduleux envoyé par un cybercriminel qui se fait passer pour un tiers de confiance (banque, administration, opérateur de téléphonie, commerce en ligne…).
2. Le corps du message, aux couleurs d'un message officiel, vous encourage à cliquer sur un lien pour réaliser une action donnée : annuler une commande, mettre à jour des données, recevoir un cadeau, obtenir un remboursement etc.
3. Lorsque vous cliquez sur le lien, vous êtes redirigé(e) vers un site Internet frauduleux reprenant les codes visuels du site Internet officiel concerné.
4. Sur le site, il vous est demandé de renseigner des informations personnelles, professionnelles et/ou bancaires.
5. Une fois les données communiquées, elles sont récupérées par des cybercriminels pour être utilisées aux dépens des victimes.

Les cybercriminels qui envoient ce message jouent sur un certain nombre de ressorts. Parmi les plus fréquents : la peur (messages anxiogènes, crainte d'une sanction de la part d'un opérateur crédible…), l'appât du gain ou de la bonne affaire (remboursement inattendu, affaire du siècle…) ou encore la crédulité des internautes (méconnaissance des risques informatiques…).

À quelles fins sont utilisées les données volées ?

Le résultat de l'exploitation de l'hameçonnage n'est pas toujours immédiat. Les conséquences d'une telle attaque peuvent en effet survenir plusieurs mois après l'incident.

Les informations dérobées par les cybercriminels sont généralement revendues sur les marchés noirs à d'autres cybercriminels. **Ces derniers utilisent alors les données obtenues pour réaliser diverses attaques : piratage de compte en ligne ou bancaire, escroquerie à caractère financier, usurpation d'identité…**

Voici quelques exemples de messages électroniques qui doivent vous alerter :

- Demande de mise à jour ou de confirmation de données personnelles suivantes : identifiants, mots de passe, coordonnées bancaires… par un prétendu organisme public ou commercial de confiance.
- Demande d'informations inattendue pour un remboursement, une annulation de commande, une livraison etc.
- Demande d'informations contre l'envoi d'un cadeau
- Demande d'informations pour participer à un jeu-concours avec un gain attrayant.
- Appel aux dons frauduleux.
- Demande de règlement pour éviter la fermeture d'un accès, la perte d'un nom de domaine ou une prétendue mise en conformité RGPD.

L'hameçonnage sur les réseaux sociaux tend également à se développer, car il permet souvent de contourner la protection mise en place par les opérateurs de messagerie. On voit ainsi y fleurir de faux bons d'achats pour des grandes surfaces, des places gratuites dans des parcs d'attractions ou bien des billets gratuits de compagnies aériennes.

Le point commun entre tous ces messages **: ils vous demandent des données personnelles** en vous attirant sur un site internet illégitime.

Il n'existe pas de liste exhaustive recensant toutes les tentatives d'arnaques par hameçonnage existantes. De nouvelles arnaques sont créées chaque jour et les cybercriminels redoublent de créativité pour mettre au point de nouveaux stratagèmes.

Voici cependant les identités les plus susceptibles d'être empruntées :

- Les banques
- Les opérateurs télécoms
- Les fournisseurs d'énergie
- Les systèmes de paiement en ligne
- Les réseaux sociaux
- Les sites de commerce en ligne
- Les administrations comme le Trésor public (les impôts), la Sécurité sociale (ameli), la Caisse d'assistance familiale (Caf), etc.
- Les services de messagerie et stockage en ligne (Cloud)
- Les sociétés de livraison

Attention : cette liste n'est pas exhaustive !

Les méthodes employées dans le cadre de ce type d'attaque sont de plus en plus sophistiquées, tandis que nous prenons l'habitude de confier parfois plus que de nécessaire nos données à des services en ligne.

https://www.dailymotion.com/video/x6xly0i

PREVENTION : APPRENDRE A REPERER LES ARNAQUES PAR MESSAGE ELECTRONIQUE

Il arrive que vous soyez tenté(e) de cliquer sur le lien d'un message, la pièce jointe d'un courriel ou de fournir vos données personnelles, car la demande semble fondée et l'identité de l'expéditeur légitime.

C'est pourquoi, il est important d'apprendre à **repérer les arnaques, et ce, avant même de cliquer sur le lien contenu dans le message.**

Voici quelques éléments que vous devez observer avec attention :

- **Le corps du texte**. L'apparence du courriel est souvent très similaire à celui des courriels officiels… mais vous pouvez déceler dans le corps du message d'éventuelles fautes d'orthographe, de grammaire ou de syntaxe, des maladresses linguistiques, des formules peu utilisées comme "Cher client", etc.

Attention : les tentatives d'hameçonnage sont de mieux en mieux réalisées et les fautes de français sont moins présentes qu'autrefois dans ces courriels (emails) frauduleux.

- **L'adresse de messagerie de l'expéditeur**. Elle est souvent différente de ce à quoi elle devrait ressembler. Observez notamment avec attention le nom de domaine, c'est-à-dire la partie de l'adresse de messagerie à droite du caractère @. Un organisme ou une grande entreprise vous adressera toujours un message émis depuis son nom de domaine (exemple : XY@entreprise.fr et non pas entreprise@XY.com).

- **Le lien**. Soyez vigilant avant de cliquer sur le lien proposé dans le message. S'il est frauduleux, il vous redirigera vers un site dont l'adresse n'est pas celle du site officiel ! Pour lever le doute, réalisez une comparaison :

1. Dans l'email, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance.
2. Rendez-vous ensuite sur le site officiel de l'organisme prétendument expéditeur de l'email, en passant par un moteur de recherche.
3. Comparez les deux adresses.

Attention : il est parfois extrêmement difficile de repérer la différence entre l'adresse frauduleuse et l'adresse légitime. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper.

Vous n'avez rien repéré de suspect dans l'email mais vous avez encore un doute quant à la fiabilité de l'expéditeur ?

Le meilleur moyen pour ne pas tomber dans le piège de l'hameçonnage est **de taper manuellement l'adresse du site officiel** dans la barre de recherche plutôt que de cliquer sur le lien contenu dans l'email. Si vous vous rendez fréquemment sur ce site, utilisez la fonction « favoris » de votre navigateur.

En vous connectant à votre espace sécurisé, vous verrez si l'organisme vous a véritablement sollicité(e) ou non.

Dernière solution : **contactez directement l'organisme concerné pour confirmer le message ou l'appel que vous aurez reçu.**

Le recours à certaines bonnes pratiques de sécurité numérique renforcent la protection de vos données et limitent ainsi les risques liés à l'hameçonnage.

- **Bien gérer vos mots de passe**. Veillez à utiliser des mots de passe différents et complexes pour chaque site et application que vous utilisez. Ainsi, le vol de l'un de vos mots de passe ne pourra pas compromettre l'ensemble de vos comptes personnels. Vous pouvez utiliser gestionnaires de mots de passe comme KeePass pour stocker de manière sécurisée vos différents mots de passe.

- **Activer la double authentification**. Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent un code provisoire que vous pouvez recevoir, par exemple, par SMS sur votre téléphone mobile ou qui peut être généré par une application ou une clé spécifique que vous contrôlez. Lorsque l'option est proposée par le site, n'hésitez pas à l'activer afin de sécuriser vos accès.

- **Vérifier les dernières connexions**. Lorsque cela est possible, vérifiez les dates et heures des dernières connexions à votre compte afin de repérer d'éventuels accès illégitimes.

  https://www.dailymotion.com/video/x7nwhwd
  https://www.dailymotion.com/video/x6x85yy

VICTIME D'ARNAQUES PAR MESSAGE ELECTRONIQUE : COMMENT REAGIR ?

Il arrive que, malgré les précautions, l'on réponde à une demande par courriel qui semblait légitime. Dans ce cas, voici les premiers réflexes à adopter :

- si vous avez envoyé **un mot de passe**, changez-le immédiatement sur le site usurpé et partout où vous l'auriez utilisé.
- si ce mot de passe concerne votre mot de passe d'adresse de messagerie, changez immédiatement votre mot de passe de messagerie ainsi que tous les mots de passe des comptes connectés à l'adresse de messagerie concernée.
- si vous avez transmis **des informations bancaires** ou si vous constatez **des débits frauduleux** sur votre compte, faites opposition à votre carte et déposez une plainte au commissariat de police ou à la gendarmerie la plus proche.
- de même, déposez plainte si vous constatez que **des éléments personnels servent à usurper votre identité**.

Si vous avez repéré l'arnaque avant d'envoyer vos données personnelles, celles-ci ne sont a priori pas en danger.

Enfin, notre dernière recommandation vaut à chaque fois que vous faites face des tentatives d'arnaques par message électronique : **signalez-les !** Pour cela, utilisez la plateforme de signalement Signal Spam. Vous pouvez ainsi contribuer à stopper les arnaques par hameçonnage et éviter que de nombreuses personnes se fassent piéger.

Une fois que vous aurez entrepris les démarches nécessaires et noté toutes les informations utiles relatives au message d'arnaque (comme l'adresse de messagerie de l'expéditeur, etc.), veillez **à supprimer le message** de votre système de messagerie.

En cas de doute ou de problème persistant concernant la sécurité de vos données, n'hésitez pas à solliciter l'aide de spécialistes. Pour être conseillé dans vos démarches, contactez la **plateforme Info Escroqueries** du ministère de l'Intérieur au 0 805 805 817 (numéro gratuit). Le service est ouvert de 9h à 18h30 du lundi au vendredi.

CONCLUSION

Il est essentiel de se tenir informé pour comprendre et éviter le risque d'arnaques par hameçonnage. N'hésitez pas **à expliquer les principes de précaution à vos proches, enfants, etc**.

Notre dernier conseil : restez vigilant(e) ! Les pratiques évoluent rapidement. Vous savez désormais comment vous prémunir et réagir en cas d'arnaques via messages électronique, mais des escroqueries similaires se déploient sur d'autres médias, comme les appels téléphoniques.