La minute du PSIR

9 Juin 2021 - # 25

Détecter un message malveillant

L'HAMEÇONNAGE ou PHISHING

NIVEAU DE DIFFICULTÉ

PHISHING

PERSONNES CONCERNÉES

Chaque jour d'innombrables courriels d'hameçonnage sont envoyés à des victimes sans méfiance dans le monde entier. Certains d'entre eux apparaissent si bizarres qu'ils sont faciles à identifier. A l'inverse, d'autres peuvent être plus convaincants. Alors, comment faire la différence entre un message de phishing et un message légitime ?

Voici nos conseils pour les repérer et surtout éviter d'en devenir victime

- **Le message comporte une URL bizarre :**

Une des premières choses à vérifier est l'intégrité et la cohérence de toutes les URLs présentes. Souvent l'URL dans un message de phishing apparaît parfaitement valable. Toutefois, si vous passez votre souris au-dessus de l'URL, vous devriez voir l'adresse réelle du lien hypertexte. Si l'adresse du lien hypertexte est différente de l'adresse qui est affichée en clair, alors il y a une forte probabilité que le message soit frauduleux ou malveillant.

- **Le mail contient des fautes d'orthographe ou de grammaire :**

Chaque fois qu'une grande entreprise envoie un message au nom de la société dans son ensemble, le message est généralement vérifié au niveau, entre autres, de l'orthographe, de la grammaire et de la légalité. Donc, si vous recevez un message rempli de fautes de grammaire ou d'orthographe, il a très peu de chance qu'il émane du département juridique d'une grande société.

- **Le message vous demande des informations personnelles**

Peu importe à quoi un courriel officiel pourrait ressembler, c'est toujours un mauvais présage si le message vous demande des renseignements personnels. Votre banque n'a pas besoin de vous pour connaître votre numéro de compte ! C'est elle qui vous l'a attribué. De même, une entreprise digne de confiance ne réclamera jamais votre mot de passe, votre numéro de carte de crédit, ou la réponse à une question de sécurité par e-mail.

- **L'offre contenue dans le mail est trop belle pour être vraie**

Il y a un vieil adage qui dit que si quelque chose semble trop beau pour être vrai, alors ça l'est probablement. Ceci est particulièrement vrai pour les messages électroniques. Si vous recevez un message d'une personne inconnue qui fait de belles promesses, c'est probablement d'une arnaque.

- **On vous demande d'envoyer de l'argent pour payer des frais**

Un signe révélateur d'un courriel d'hameçonnage est qu'on finit par vous demander de l'argent. Il est possible qu'on ne vous demande rien dans le message initial. Mais tôt ou tard, les escrocs au phishing vont probablement vous demander de l'argent pour couvrir des frais, taxes, redevances, ou quelque chose de semblable. Si cela se produit, vous pouvez être quasiment certain qu'il s'agit d'une arnaque.

- **Le message vous adresse des menaces irréalistes**

Bien que la plupart des escroqueries par phishing tentent de tromper les gens en leur demandant de l'argent ou des informations sensibles en leur promettant des gains d'argent instantanés, certains artistes de l'hameçonnage utilisent l'intimidation pour effrayer les victimes en donnant des informations. Si un message fait des menaces irréalistes, il s'agit probablement d'une arnaque.

Si des doutes persistent,
sollicitez-nous en nous communiquant le mail en pièce-jointe

Vous trouverez ci-dessous un petit jeu pour tester votre vigilance : un quiz ludique destiné à tous permettant de tester vos réflexes face aux mails de phishing. En 8 exemples interactifs, vous devez identifier quels mails sont légitimes et lesquels sont des tentatives d'hameçonnage (Faux email pour récupérer vos données, pièces jointes piégées, etc). Les principaux exemples de mises en scènes sont représentés et sont loin d'être si évidents à identifier.

Faites le Test