Le Hameçonnage (phishing)

Apprenez à repérer les mails et SMS frauduleux en 3 étapes clés.

Difficulté	Public	Licence	Type de contenu
Facile	Grand public	CC-BY-SA	Mediation

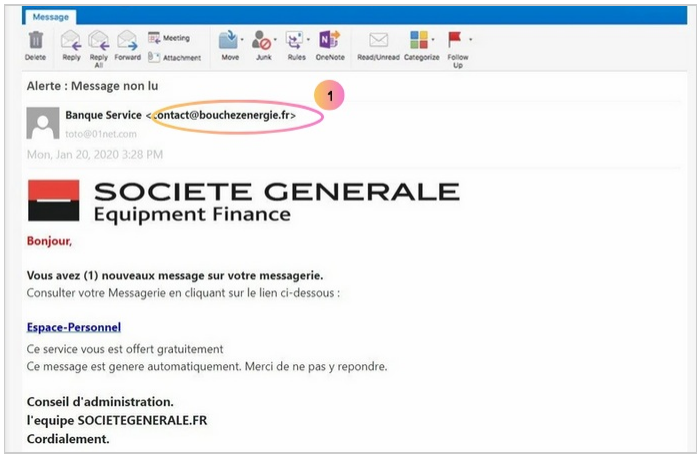
Sommaire

Introduction

Le hameçonnage, c'est pour une personne malveillante de **se faire passer pour un organisme qui vous est familier** (banque, CAF, opérateur de téléphonie, impôts, etc) en utilisant son logo, son nom.
Objectif : Dérober des informations personnelles et/ou financières.
Comment : Faux mail ou SMS

Voici les 3 méthodes simple pour repérer un mail frauduleux.

Étape 1 - Vérifier l'adresse mail de l'expéditeur



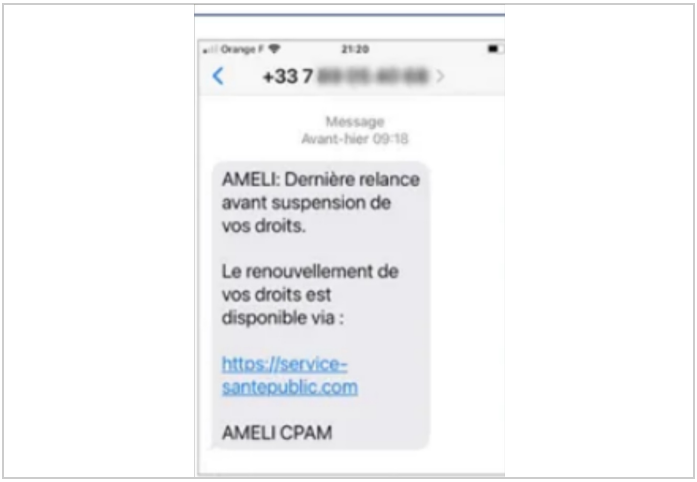
Sur ce mail, le logo ne correspond pas du tout à l'adresse mail indiqué en haut du mail. L'expéditeur n'est donc pas la Société Générale. Il est important de regarder ce qui se trouve après le @ dans une adresse mail.

Lorsqu'une grande entreprise ou administration vous contacte par mail, la fin de l'adresse doit correspondre à son nom ; ici l'adresse devrait terminer par "....@socgen.com".

D'autres exemples :
....@impots.gouv.fr
....@boursorama.fr
....@doctolib.fr

> Il n'est pas rare de voir la mention "no-reply" (anglais) ou bien "ne-pas-repondre" dans une adresse mail. Cela signifie que le mail est envoyé automatiquement et qu'il ne faut pas y répondre.

Étape 2 - Vérifier le ton du mail ou du SMS



Le ton du mail donne un indice important sur sa véracité. S'il paraît urgent, stressant, trop beau pour être vrai ou bien qu'il fait peur, il y a de grandes chances que ce soit un mail frauduleux.

L'objectif de la personne malveillant est de vous mettre dans un état de stress ou d'euphorie pour que vous cliquez rapidement sur un lien contenu dans le mail afin de vous piéger.

Exemples de tournures de phrases dans un mail frauduleux

Urgence :
- "Vous avez 24h pour cliquer sur ce lien, sinon vous perdrez tous vos avantages."
- "Vous avez été tiré au sort, cliquez dans les 10 minutes pour recevoir votre cadeau"

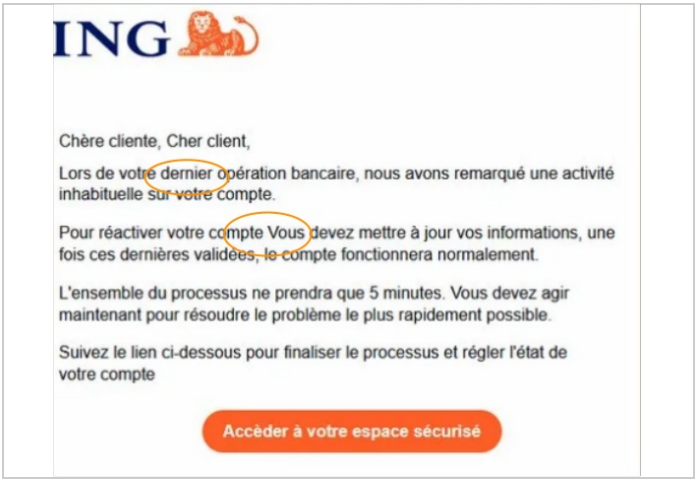
Peur :
- "Dernière relance avant suspension provisoire de vos droits d'assurance maladie"
- "Si nous ne recevons pas de confirmation d'ici 2 jours, nous serons dans l'obligation de suspendre votre carte bancaire"

Le faux gain ou cadeau :
- "Black Friday ! Offre exceptionnelle dans votre boutique, le tout nouveau smartphone à -90%"
-" Félicitations ! Vous venez de remporter une carte cadeau de 500€ !"

Au contraire, un vrai mail n'est pas urgent et ne vous pousse pas à l'action de manière forcée.

> En cas de doute, ne pas ouvrir les pièces jointes ni cliquer sur les liens. Vous pouvez tout de même lire le mail.

Étape 3 - Vérifier l'orthographe



Cette méthode tend à disparaître, en effet les mails frauduleux sont de mieux en mieux rédigé. Mais si vous êtes à l'aise, repérer quelques fautes d'orthographe pourra vous aider à déceler un faux

Étape 4 - Conclusion : les bonnes pratiques

- Vérifier l'expéditeur du mail, le ton et l'orthographe
- Est-ce que le message m'est réellement destiné ?
- Avant de cliquer sur un lien contenu dans un mail, positionnez le curseur de votre souris dessus afin de voir le site sur lequel il renvoie
- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone :
- Aucune administration ou société sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.
- En cas de doute, contactez directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.