PHISHING : VIGILANCE !

LE PHISHING, DE QUOI S'AGIT-IL ?

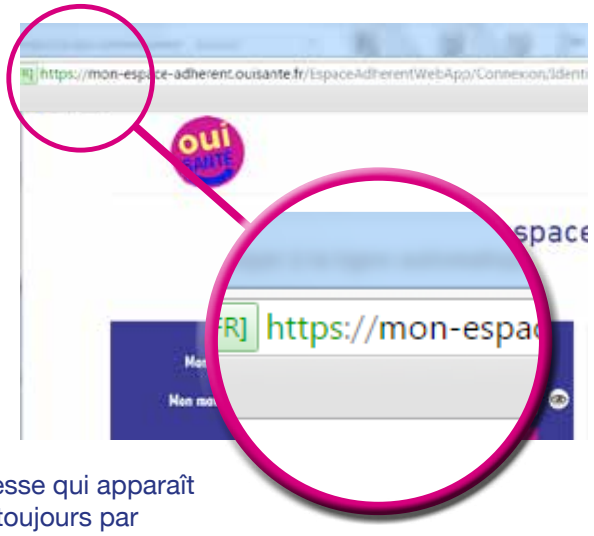
Le phishing, ou hameçonnage, est une **technique frauduleuse** destinée à récupérer des données personnelles sur internet. Elle consiste à **usurper l'identité de votre mutuelle** ou de tout autre organisme familier, par exemple votre banque, en utilisant son logo et son nom. Un courriel vous invite sous divers prétextes (« mise à jour », « incident technique ») à cliquer sur un lien hypertexte ou à remplir un formulaire pour confirmer vos coordonnées bancaires, identifiants et mots de passe. Une fois saisies, ces informations sont récupérées et peuvent être utilisées pour effectuer des transferts d'argent depuis votre compte par exemple.

COMMENT RECONNAÎTRE UN COURRIEL FRAUDULEUX ?

Aucun organisme de confiance n'enverra jamais un courriel pour vous demander de saisir vos données personnelles par ce biais. Les courriers frauduleux ne sont généralement pas ciblés et souvent rédigés dans un français approximatif. La plupart du temps l'expéditeur du message n'est pas visible ou différent du domaine de l'organisation à laquelle il est censé appartenir. Si l'adresse du lien hypertexte est également différente, c'est un indice supplémentaire de fraude. Pour le vérifier, il suffit de pointer votre souris sur le lien, sans cliquer dessus, pour voir l'adresse s'afficher en bas à gauche de votre navigateur Web.

UN DOUTE ?

Posez-vous les bonnes questions : *« Ai-je communiqué mon adresse de messagerie à ma mutuelle ? » « Le courrier possède-t-il des éléments personnalisés qui permettent de vérifier sa véracité, par exemple mon numéro d'adhérent ? » « Mon agence ou ma banque est-elle au courant ? »* **Dans le doute, contactez-les directement.** D'une manière générale, soyez extrêmement vigilant. Ne répondez jamais à un courriel qui vous demande de communiquer vos données personnelles.



COMMENT ÊTRE SÛR DE SAISIR MES INFORMATIONS PERSONNELLES SUR LE SITE DE OUI SANTÉ ?

Sur ouisanté.fr, aucune information ne vous sera demandée. Concernant l'espace adhérent **OUI SANTÉ**, **le site est sécurisé :** l'adresse qui apparaît dans le navigateur (la barre qui affiche l'adresse du site) commence toujours par « **https** » au lieu de « http ». De plus, le navigateur indique d'une **couleur verte que l'accès est valide**. Par ailleurs vous retrouverez **obligatoirement** « **ouisante.fr** » dans les adresses des sites concernés (et non pas, par exemple, « ouisant.net », ou « ouysante.fr »).

Ce qu'il faut retenir

- Le phishing est une technique frauduleuse destinée à récupérer vos données personnelles pour usurper votre identité et vous escroquer.
- Ne jamais répondre à un mail qui vous demande de les communiquer.
- Quand vous saisissez en ligne des informations sensibles, vérifiez que l'adresse dans la barre du navigateur commence par « https » précédé d'un cadenas. D'une manière générale, être vigilant et faire preuve de bon sens : ne pas croire que ce qui vient d'Internet est forcément vrai.
- En cas de réception d'un e-mail suspicieux, l'envoyer à **nous-contacter@lamutuellegenerale.fr**