Fwd: [ATTENTION AUX FAUX EMAILS]

Boîte de réception x

De : SERVICE ASSISTANCE <assist@site-paris.fr> (envoyé par bgential@site-paris.fr)
À : collaborateurs

Le Service Assistance vous informe

Les tentatives de phishing ou hameçonnage par email continuent. Elles ciblent notamment les banques, les opérateurs Télécom et tous les fournisseurs de messagerie en ligne. Voici quelques moyens pour vous permettre d'identifier les messages falsifiés vous invitant à communiquer vos informations personnelles (identifiant et mot de passe, numéro de carte bancaire ...). Si vous recevez un message de phishing ou avez répondu en communiquant vos informations, veuillez prévenir sans délai le 75.17.

1. N'ayez pas une confiance aveugle dans le nom de l'expéditeur ou la présentation du courrier électronique

N'importe qui peut vous envoyer un courriel en se faisant passer pour un autre !

Il peut s'agir en apparence, d'une personne que vous connaissez (collaborateur, ami, proche...), mais l'usurpation d'identité dans les messageries électronique n'est pas beaucoup plus compliquée que de mettre un faux nom d'expéditeur au verso d'une enveloppe papier.

Soyez donc attentif à tout indice mettant en doute l'origine réelle du courriel, notamment si le message comporte une pièce jointe ou des liens.

Surveillez les incohérences de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d'habitude. Les fautes d'orthographe et les erreurs de syntaxe sont également des indices à considérer.

En cas de doute, contactez votre interlocuteur pour vérifier qu'il est bien à l'origine du message.

Et même si l'expéditeur est le bon, il a pu, à son insu, vous envoyer un message infecté. De la même manière, la présence de logos ou d'éléments graphiques (un service support, une entité renommée...) dans le message n'apporte aucune garantie sur la fiabilité de sa provenance.

2. Ne répondez jamais à une demande d'informations confidentielles

Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.). En cas de doute, là encore, demandez à votre correspondant légitime de confirmer sa demande.

Car vous pouvez être victime d'une tentative de hameconnage ou de phishing. Il s'agit d'une technique utilisée par des personnes malveillantes, usurpant généralement l'identité d'un tiers ou simulant un site dans lesquels vous avez a priori confiance (une banque, un site de commerce, etc.) dans le but d'obtenir des informations confidentielles, puis de s'en servir frauduleusement.

Les messages du type chaîne de lettres, porte-bonheur ou pyramide financière, appel à solidarité, alerte virale, ou autres, peuvent cacher une tentative d'escroquerie. Évitez de les relayer, même si vous connaissez l'expéditeur.

3. Méfiez-vous des pièces jointes, des liens cliquables et des fausses interfaces

Les pièces jointes peuvent contenir des virus informatique ou des logiciels espion. Ne les ouvrez que si elles sont en rapport avec le message et votre activité en ayant pris soin de vérifier au préalable que votre anti-virus était à jour et actif.

Les liens cliquables représentent la plus grande menace ; ils sont largement utilisés pour tromper la vigilance des internautes.

Vous pouvez vérifier leur validité en passant la souris au-dessus du lien proposé et repérer s'il pointe bien vers l'adresse du site annoncé dans le message.

Si l'adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur.

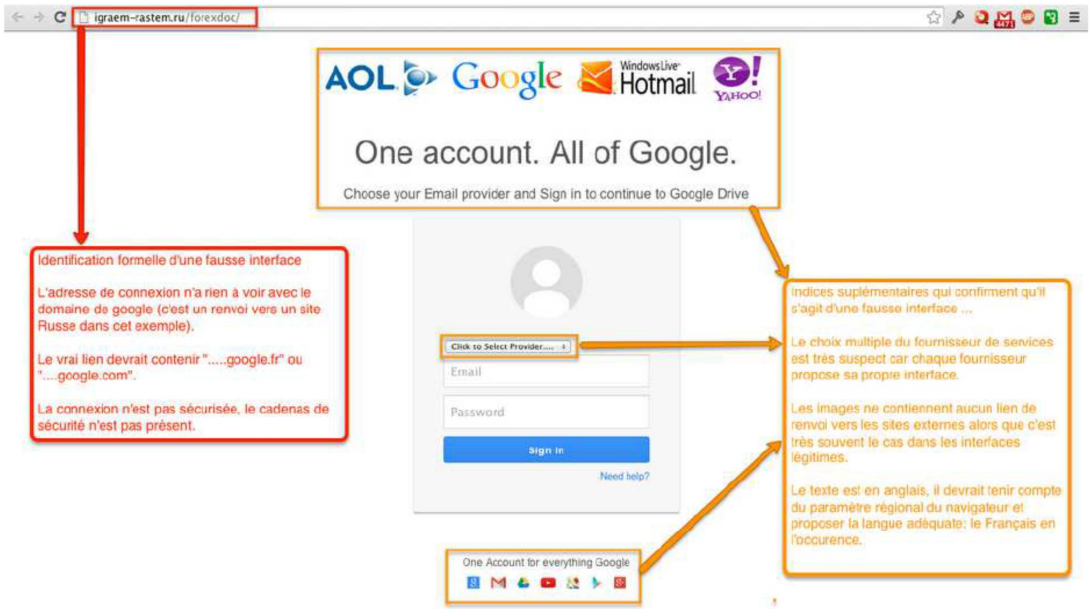
Les fausses interfaces se multiplient, elles ressemblent à s'y méprendre aux sites originaux, soyez vigilants avant de saisir vos identifiants.

Pensez à vérifier :

- si l'adresse URL indiquée par le navigateur est bien associée au domaine auquel vous vous connectez,

- si la présence d'un cadenas qui indique que la liaison avec le serveur est sécurisée.

Exemple d'une fausse page



Le Service Assistance 7517 (7517@site-paris.fr) reste à votre disposition pour toute information complémentaire.

Bien cordialement,

Service Assistance 7517
Direction du Système d'Information
Site Paris
Tél : 75.17 (8h00-19h00)
Mail : 7517@site-paris.fr