

Nous vous aidons à lutter contre le phishing.

Guide anti-phishing de Retarus

Contre les e-mails de phishing qui atterrissent dans votre boîte de messagerie, il existe encore un rempart : vous-même.

Découvrez comment vous protéger de la fraude en ligne de manière optimale.



Soyez vigilant.

Méfiez-vous des tentatives de fraude en ligne à tout moment. Vos chances de « mordre à l'hameçon » seront ainsi grandement réduites.

i Le phishing est une forme de fraude en ligne : des cybercriminels tentent de propager des programmes malveillants, de s'approprier des données et d'en tirer un profit. Pour ce faire, ils utilisent de fausses identités et diffusent des messages trompeurs qui visent à profiter de qualités ou faiblesses humaines : la crédulité, la générosité ou la peur (ingénierie sociale).



Les cybercriminels usurpent volontiers l'identité de proches.

Le phishing conduit par les cybercriminels se font passer pour des amis, membres de la famille, collègues, supérieurs hiérarchiques ou partenaires commerciaux. Ils s'adressent également à vous comme s'ils agissaient au nom d'établissements officiels, de services financiers connus ou encore de portails en ligne (votre banque, PayPal ou Amazon, par exemple).



Ainsi, quand bien même vous pensez connaître l'expéditeur d'un e-mail, il peut s'agir en fait d'une tentative de phishing.

La qualité du phishing augmente : techniquement, sur le fond et sur la forme.

Les e-mails de phishing comportant des liens obscurs et interminables, écrits dans un français approximatif et présentant un design médiocre se font de plus en plus rares. Aujourd'hui, ces e-mails sont techniquement sophistiqués, bien formulés et conçus de manière professionnelle.



Les e-mails falsifiés ainsi que les expéditeurs, les pièces-jointes, les fichiers à télécharger et les sites Web frauduleux semblent authentiques. Même en y regardant à deux fois, on ne se rend pas toujours compte qu'ils sont faux.

Agissez avec circonspection.

Si vous avez l'impression qu'un e-mail ou un site Web a l'air suspect, faites preuve de retenue. Face à une attaque de type phishing, la meilleure chose à faire est de ne rien faire.

i Les cybercriminels cachent des programmes malveillants (malware) dans les pièces jointes, les liens et les fichiers à télécharger. Ceux-ci peuvent paralyser votre ordinateur et, dans le pire des cas, toute l'infrastructure informatique.



-
- #1** Ne cliquez jamais sur les liens contenus dans des e-mails suspects (même les liens de désabonnement*).
-
- #2** N'ouvrez pas et ne téléchargez pas les pièces jointes d'e-mails suspects (malware).
-
- #3** Ne répondez pas* à un e-mail suspect et ne le transférez pas.
-
- #4** Ne divulguez jamais des noms d'utilisateur, des mots de passe ou d'autres informations personnelles sur les sites Web suspects.
-

*cela ne ferait que confirmer votre adresse e-mail

Attention à la « fraude au président » (CxO Fraud) !

La « fraude au président » (CxO Fraud) est une méthode d'hameçonnage particulièrement audacieuse : des cybercriminels se font passer pour des dirigeants de l'entreprise et usent de faux prétextes (par exemple, une situation d'urgence) pour pousser des employés à commettre certains actes (par exemple, une transaction financière ou la divulgation d'informations confidentielles).

L'extrême urgence et la demande de traitement confidentiel sont typiques des e-mails d'hameçonnage de ce genre.

Vous connaissez l'expéditeur d'un e-mail au contenu douteux ?

Vérifiez l'authenticité de l'e-mail en vous adressant personnellement à l'expéditeur ou en l'appelant.

Vous pensez être tombé dans un piège de phishing ?

N'hésitez pas une seconde : informez-en vos supérieurs hiérarchiques et/ou vos collègues du département informatique. Ils sauront comment réagir.

Soyez méfiant.

Les cybercriminels s'engouffrent dans tout ce qui émeut et concerne directement les personnes. Les sujets qui nous touchent personnellement, qui sont massivement couverts par les médias, qui nous préoccupent ou nous réjouissent constituent des leurres d'hameçonnage «rêvés» pour les malfrats du net.



Faites attention ! Les escrocs n'utilisent pas seulement les e-mails et les sites Web : ils agissent aussi sur les réseaux sociaux, par SMS ou par téléphone. Ils peuvent même se présenter à votre porte.



C'est pourquoi le premier conseil à donner est d'être méfiant lorsqu'une offre « tombe à pic », lorsqu'un message semble vous concerner particulièrement, ou lorsqu'il s'agit d'instructions relatives au télétravail. Prenez un moment, observez les pensées et les sentiments qu'un message déclenche en vous. Est-ce qu'une routine, un principe, une règle générale vous « guide » ? Une autorité vous « parle » ? Avez-vous peur ? Est-ce que cette opportunité qui se présente à vous semble trop parfaite pour être vraie ? Si c'est le cas, respirez profondément, réfléchissez à nouveau, faites éventuellement quelques recherches complémentaires et ne réagissez qu'ensuite. Ou ne réagissez pas.

Par quels biais les cybercriminels tentent-ils de propager des programmes malveillants, de s'approprier des données et de gagner de l'argent ?

Informations officielles, indispensables ou exclusives, disponibles via un abonnement à une newsletter, en pièce jointe d'e-mail ou en fichier à télécharger

Opportunités uniques telles que des offres sur des produits à forte demande ou disponibles seulement pour une durée limitée, des chances de gain élevées, des conseils d'investissement intelligents, ...

Requêtes/couplage de données de comptes en ligne (collaborateurs, clients, utilisateurs, membres, patients, ...)

Instructions et demandes qui **exercent une pression** sur le lecteur (des situations d'urgence, des omissions, des dangers, ...)

Téléchargements ou installations de logiciels ou de mises à jour de sécurité

Demandes de mot de passe pour la participation à une vidéoconférence

Requêtes/couplage de données en vue de l'activation d'un outil à distance (télémaintenance)

Une consigne du département informatique en lien avec le télétravail vous semble suspecte ?

N'hésitez pas à demander confirmation auprès du département informatique.

La seule véritable solution contre le phishing : une bonne sécurité de la messagerie alliée à votre bon sens !

Soyez vigilant : méfiez-vous des tentatives de fraude en ligne à tout moment. Agissez avec circonspection : évitez les clics et téléchargements hâtifs. Soyez méfiant : remettez en question les informations, faites preuve de bon sens et utilisez plusieurs sources d'information.

Retarus Email Security

Pour que les e-mails soient un levier et non un frein à l'entreprise.

retarus.fr/email-security

