Phishing

*Une technique d'attaque consistant à **envoyer un e-mail** (ou SMS) copiant ceux provenant d'une entreprise que la cible connait et contenant **un lien** ou **une pièce jointe** dans le but d'obtenir **des informations confidentielles** ou **d'introduire un code malveillant.***

Comment se protéger ?

Réfléchir avant de cliquer

En présence d'un lien à cliquer ou d'une pièce-jointe à télécharger, toujours prendre le temps d'étudier le message attentivement.

Examiner l'adresse de l'émetteur

Vérifier l'émetteur du message, il suffit parfois d'une seule lettre de différence pour vous tromper. En cas de doute, contactez directement l'organisme ou la personne que vous connaissez pour obtenir confirmation.

Se méfier des pièces jointes

N'ouvrez que celles que vous attendez ou vérifiez auprès du correspondant que vous connaissez qu'il s'agit bien d'un envoi de sa part.

Passer la souris sur le lien

Lorsque vous recevez un mail qui contient un lien sur lequel il vous est demandé de cliquer, pointez votre souris dessus sans cliquer. Cela vous donnera la véritable destination du lien.

Recopier plutôt que cliquer

Vous pouvez aussi copier ce lien dans votre barre de navigation, ainsi la destination correspondra bien au texte que vous lisez.

Urgence : méfiance !

Si on vous presse de réaliser une action de façon immédiate et urgente, méfiez-vous.

Un œil sur l'orthographe

Vérifiez l'orthographe.

Email pro à des fins pros

Utilisez votre adresse mail professionnelle UNIQUEMENT pour un usage professionnel.

Le phishing est un business très lucratif.

Ce type **d'attaques** a explosé **ces dernières années**, avec

66 %

des malwares désormais installés **via une pièce jointe malveillante.**

85 % des entreprises** ont été victimes **d'une attaque de phishing au moins une fois.

*Environ **1,5 million de nouvelles URL de phishing** sont identifiées **chaque mois.***

Les attaques avancées de phishing coûtent aux entreprises en moyenne $140 000 par incident.

GCSeara la santé connectée