7 SIGNES QUE VOUS ÊTES VICTIME DE PHISHING !

Certains signes d'alerte courants d'un e-mail de phishing potentiel.

L'e-mail est mal écrit

Bien que les escrocs puissent accidentellement faire des fautes de grammaire, ces "erreurs" ne sont pas toujours involontaires. Les erreurs peuvent être incluses délibérément afin de limiter l'interaction avec les personnes les plus " observantes ".

Il contient des pièces jointes non sollicitées

En général, les vraies entreprises n'envoient pas d'e-mails avec des pièces jointes au hasard, surtout lorsqu'il n'y a pas de relation antérieure. En cas de doute, contactez la société en recherchant son site Web.

Il demande des informations sensibles

Les e-mails qui vous demandent d'envoyer des informations sensibles, telles que des coordonnées bancaires, des relevés d'impôts ou des identifiants de connexion, sont très malveillants. Vous devez effectuer des recherches en ligne et contacter directement l'organisation, et non l'expéditeur.

Il y a urgence à agir

Certains escrocs tentent d'imposer l'urgence dans leurs e-mails - souvent avec des menaces d'expiration de compte, d'amendes ou même de prix à gagner - pour nous inciter à prendre des décisions irréfléchies.

Ça semble trop beau pour être vrai.

Les escrocs incluent souvent des prix " limités " et " incontournables " dans leurs e-mails de phishing pour tenter tromper les utilisateurs. C'est quoi déjà le vieil adage ? "Si cela semble trop beau pour être vrai...".

Il ne s'adresse pas à vous par votre nom

De nombreuses escroqueries par phishing sont envoyées en masse, sans personnalisation (ou avec une personnalisation limitée).

L'adresse e-mail semble modifiée

Les escrocs peuvent faire passer leur adresse électronique pour légitime en incluant le nom de l'entreprise dans la structure de leur courrier électronique (par exemple john@paypal123.com). Passez la souris sur les liens pour vous assurer qu'ils ne sont pas altérés.