STOP ! RÉFLÉCHISSEZ AVANT D'AGIR !

Le phishing, appelé aussi hameçonnage, pourrait bien représenter la plus grande menace pour la sécurité des entreprises dans le monde. Mais il peut être contré grâce à votre vigilance. Réfléchissez avant d'agir !

Phishing exploite une ressemblance avec une entreprise ou une personne spécifique pour piéger les employés et les amener à révéler des informations confidentielles. Il se présente sous différentes formes – par e-mail, téléphone et réseaux sociaux.

✓ Faire

Utilisez des filtres
Utilisez des filtres de courrier indésirable et des protections à jour.

Soyez prudents
Faites preuve de prudence vis-à-vis de toutes les pièces jointes à un e-mail, quelle que soit la personne qui semble les avoir envoyées.

Vérifiez les liens
Survolez les liens avec le curseur de la souris afin de vérifier qu'ils dirigent bien vers les bonnes URL d'un site web.

Vérifiez les contacts
Vérifiez l'identité des contacts en contrôlant leurs adresses e-mail et numéros de téléphone.

Faites attention
Faites attention aux réponses des réseaux sociaux à vos demandes : elles peuvent provenir de comptes frauduleux.

⊘ Ne pas faire

Ne cliquez pas
Ne cliquez pas sur des liens ou des pièces jointes dont vous ne connaissez pas l'expéditeur.

N'ouvrez pas
Ne répondez pas aux messages suspects et inhabituels.

Ne répondez pas
Ne répondez jamais aux demandes d'informations personnelles ou de codes d'accès.

Gardez vos secrets
Ne divulguez jamais vos informations bancaires ; conservez à l'abri le code PIN et le code de sécurité de votre carte bancaire.

Évitez les pop-ups
Ne cliquez pas sur les pop-ups car ils pourraient vous rediriger vers un site frauduleux ou lancer le téléchargement d'un logiciel malveillant.