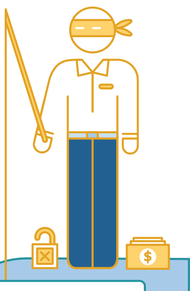
Repérez les tentatives d'hameçonnage. Protégez votre entreprise.

Qu'est-ce que l'hameçonnage?



L'hameçonnage est une technique par laquelle les cybercriminels envoient de faux courriels, messages textes ou sites Web qui ressemblent à s'y méprendre à une correspondance légitime afin de tromper les employés et d'accéder aux systèmes informatiques ou aux renseignements de l'entreprise.

Principales caractéristiques :

- Tente d'inciter une réaction rapide de votre part;
- Fournit un lien vers un site Web distinct;
- Vous demande généralement de « mettre à jour », de « valider » ou de « confirmer » des renseignements personnels;
- Imite souvent un expéditeur officiel (par exemple, votre entreprise, le gouvernement ou une institution financière).

91%

des attaques cybernétiques commencent par une tentative d'hameçonnage[1].

65%

d'augmentation du nombre de courriels d'hameçonnage au cours de la dernière année[2].

97%

des destinataires n'ont pas réussi à distinguer un courriel d'hameçonnage d'un message légitime lors de tests[3].

Types d'hameçonnage

HAMEÇONNAGE TROMPEUR

Courriels ciblant tous les employés en empruntant l'identité d'une source reconnue ou légitime et contenant des liens malveillants.

HARPONNAGE

Courriels hautement personnalisés et faux sites Web ciblant des employés en particulier (par exemple, au service des finances).

CHASSE À LA BALEINE

Courriels hautement personnalisés et faux sites Web ciblant certains cadres supérieurs (par exemple, le PDG).

COURRIEL D'AFFAIRE COMPROMIS (CAC)

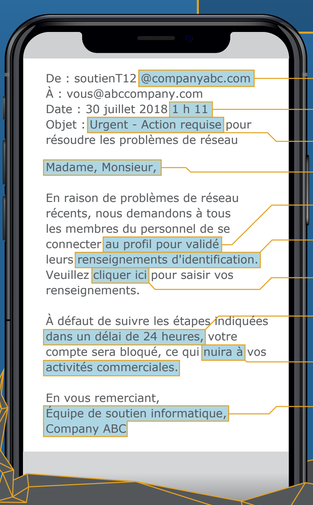
Courriel interne de l'entreprise empruntant l'identité d'un dirigeant (par exemple, le PDG).

DÉVOIEMENT

Domaines de site Web détournés redirigeant les visiteurs vers un site frauduleux.

Réfléchissez avant de cliquer!

Ce qu'il faut surveiller :



- **Expéditeur inconnu ou suspect**
- **Envoi à une heure inhabituelle**
- **Objet à caractère sensationnel et urgent**
- **Salutation générique**
- **Fautes de grammaire et d'orthographe**
- **Demande des renseignements personnels ou sensibles**
- **Ajout de liens ou de pièces jointes suspects**
- **Forte impression d'urgence ou de confidentialité**
- **Promesse d'une conséquence menaçante ou d'une récompense**
- **L'expéditeur prétend être une personne en position d'autorité**

ANCHOR
Solutions de risques

[1] "2016 Enterprise Phishing Susceptibility and Resiliency Report," Cofense. [2] "2017 Enterprise Phishing Resiliency and Defense Report," Cofense. [3] "Intel Security Study," 2015.