

Pourquoi est-ce un problème...



...si je ne sais pas à quoi ressemble un courriel d'hameçonnage?

Pourquoi est-ce un problème
<ul style="list-style-type: none">• Vous exposez le réseau électronique de notre ministère à des risques si vous vous faites piéger et que vous cliquez sur une pièce jointe ou un lien infecté. Par inadvertance, vous pourriez télécharger des logiciels espions ou malveillants.
Scénario
Vous recevez un courriel ayant pour objet « Affaire urgente » et le courriel contient un fichier PDF. Ce dernier pourrait traiter du nouveau contrat auquel vous travaillez, mais vous savez que ce fichier pourrait être un leurre. Quels sont les indices que vous devez rechercher pour déterminer s'il s'agit d'un courriel d'hameçonnage?
Mesures possibles (votez pour la bonne réponse)
<ul style="list-style-type: none">• Option 1 : Vérifier l'horodatage, le bloc de signature, les erreurs d'orthographe et de grammaire, les salutations génériques.• Option 2 : Vérifier s'il y a des petits changements aux noms de domaine du courriel.• Option 3 : Survoler le lien avec le curseur pour que s'affiche l'URL véritable.
Explication
<ul style="list-style-type: none">• Les options 1, 2 et 3 sont toutes valables! Ce ne sont que quelques-uns des indices qui peuvent vous aider à déterminer s'il s'agit d'un courriel d'hameçonnage.• Vous devez examiner tous ces éléments ensemble. Si quelque chose cloche, signalez le courriel en utilisant le bouton Outlook « Signaler ce courriel-Hameçonnage ».
Messages clés à retenir
<ul style="list-style-type: none">• Les courriels d'hameçonnage sont l'une des méthodes les plus couramment utilisées par les cybercriminels pour voler des renseignements, c'est pourquoi vous devez savoir comment reconnaître ce type de courriel.• Ouvrez les courriels provenant d'expéditeurs inconnus avec une extrême prudence. Utilisez le processus HALTE, qui vous permettra de déterminer s'il s'agit d'un courriel digne de confiance.• Si le courriel vous semble suspect, il l'est probablement! N'y répondez pas, ne cliquez sur aucun lien et n'ouvrez pas les pièces qui y sont jointes. Signalez-le immédiatement en utilisant le bouton Outlook « Signaler ce courriel-Hameçonnage ».• Si vous croyez qu'il pourrait s'agir d'un courriel authentique, mais que vous n'en êtes pas certain et que vous ne voulez pas le supprimer prématurément, vérifiez l'adresse courriel ou le numéro de téléphone de l'expéditeur au moyen d'une autre méthode (p. ex. les Services d'annuaires gouvernementaux électroniques, répertoire Outlook). Ensuite, appelez l'expéditeur ou envoyez-lui un nouveau courriel afin de lui demander si le courriel que vous avez reçu est authentique.
Pour de plus amples renseignements
<ul style="list-style-type: none">• Halte à l'hameçonnage• Pourriels et courriels d'hameçonnage