

Hameçonnage



Savez-vous comment éviter d'être piégé?

Combien de courriels ou de textos avez-vous reçus vous demandant de cliquer sur un lien pour valider votre compte ou fournir des informations personnelles? Étaient-ce des messages authentiques?

Les fraudes d'hameçonnage se font passer pour des institutions fiables et sont conçues pour provoquer une action immédiate.

Ne soyez pas dupes! Apprenez à reconnaître les signes révélateurs d'une attaque pour assurer votre protection ainsi que celle de notre organisation.

Pensez-y deux fois!

La vigilance et un bon jugement sont vos défenses les plus importantes contre les attaques d'hameçonnage.

Soyez un maillon fort!

Ne fournissez jamais d'informations personnelles en réponse à un message non sollicité et quittez immédiatement les sites Web suspects.

Méfiez-vous des courriels ou des messages textes contenant des demandes urgentes ou promettant de l'argent en échange d'informations personnelles ou confidentielles.

Assurez-vous que votre connexion est chiffrée avant de saisir toute information sensible sur un site Web. L'adresse URL devrait commencer par `https://` ou comporter un symbole de cadenas.

Accédez toujours aux sites de la manière habituelle et jamais par l'entremise d'un lien fourni dans un courriel ou message texte.