Assist identité vous rappelle :

« Protégez-vous contre les arnaques basées sur la COVID-19 »

Le 11 mars 2020, l'Organisation mondiale de la Santé (OMS) a qualifié l'épidémie de COVID-19 (maladie à coronavirus 2019) de pandémie mondiale. Les cybercriminels tirent déjà profit de la situation et exploitent cette pandémie au moyen de courriels d'hameçonnage conçus pour voler des renseignements personnels et de l'argent.

Non seulement vous devez protéger votre bien-être et celui de vos proches, mais vous devez aussi protéger votre identité en ligne pour éviter d'être victime de ces cybercrimes malveillants.

Les entreprises mettent en place des politiques temporaires de travail à domicile, les écoles ferment temporairement leurs portes, les événements sportifs sont suspendus et les grandes manifestations sont annulées ou reportées. Assist identité est là pour vous aider à protéger vos renseignements personnels et vos finances afin d'éviter de devenir victime d'une fraude d'identité.

On a découvert que des criminels distribuent des courriels d'hameçonnage en se faisant passer pour l'Organisation mondiale de la Santé (OMS) et d'autres organismes gouvernementaux afin de voler de l'argent et des renseignements personnels de nature délicate. Vous commencerez à voir (si ce n'est pas déjà fait) un nombre croissant de courriels concernant la COVID-19.

Qu'est-ce que l'hameçonnage?

L'hameçonnage est une façon frauduleuse d'obtenir des renseignements de nature délicate, comme les noms, les noms d'utilisateur, les mots de passe, les adresses et les renseignements sur les cartes de crédit d'une personne en se faisant passer pour une entité digne de confiance dans une communication électronique comme un courriel.

Voici quelques conseils pour vous protéger contre la cyberfraude :

- Assurez-vous qu'un logiciel antivirus à jour est installé sur vos appareils.
- Ignorer les communications provenant de contacts inconnus. Si la communication semble légitime, assurez-vous de vérifier attentivement l'adresse de courriel de l'expéditeur. Les fraudeurs créent souvent des adresses qui ressemblent de très près à une adresse légitime.
- N'ouvrez pas les courriels suspects, car ils peuvent contenir des virus. Supprimez-les immédiatement.
- Ne cliquez pas sur des hyperliens suspects dans les courriels, pour vérifier un hyperlien sans cliquer, placez votre souris dessus. Vérifiez-en soigneusement l'exactitude.
- Ne répondez pas aux pourriels, même pour vous désabonner, n'ouvrez pas de pièces jointes et ne suivez aucun lien. Ces éléments peuvent être porteurs de virus ou vous pourriez installer à votre insu des maliciels sur votre appareil.
- Les organisations fiables ne demanderont jamais vos renseignements personnels par téléphone, courriel ou texto.
- N'utilisez jamais le numéro de téléphone ou l'adresse électronique fournie dans un message suspect. Utilisez toujours des coordonnées provenant de sites Web vérifiés.