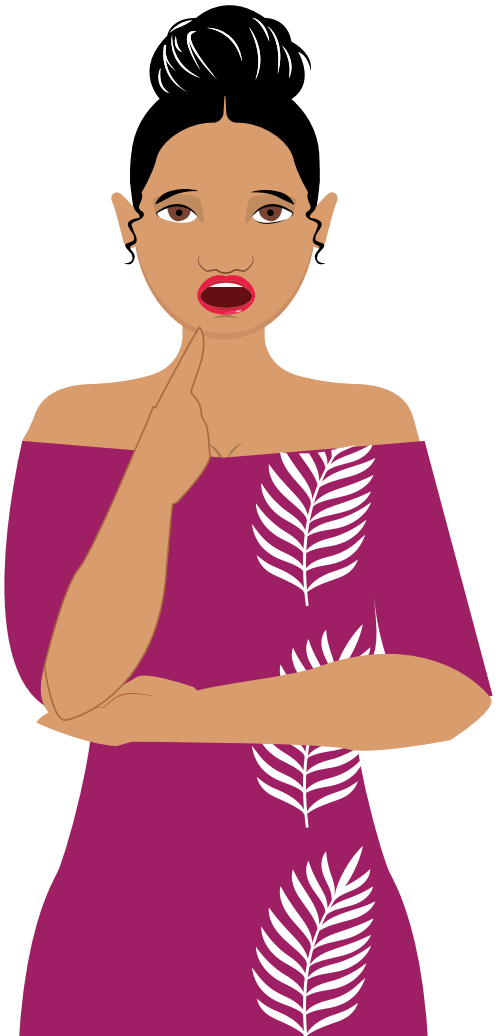
Repérer et éviter les escroqueries en ligne



Aller sur Internet pour entrer en contact avec d'autres personnes peut être amusant et enrichissant. Mais il est important de savoir que tous les contacts ou personnes ne sont pas ce qu'ils semblent être. Les escrocs peuvent être très malins et cibler n'importe qui pour essayer de vous soutirer de l'argent ou des informations personnelles ou faire de même avec l'une de vos connaissances. Il est important d'apprendre à identifier et à éviter les escroqueries afin de contribuer à notre protection ainsi qu'à celle de nos amis et de notre famille.

Types courants d'escroquerie

Les escroqueries peuvent se produire de différentes manières, notamment par le biais de courriels, de médias sociaux, d'appels téléphoniques, de SMS et même de lettres traditionnelles ou autres documents traditionnels. Les types d'escroquerie les plus courants sont les suivants :

- Les **escrocs des prix et des promotions** peuvent prétendre que vous avez gagné un prix ou une loterie et vous demander de payer ou de partager vos informations personnelles pour le recevoir - mais en fait, ce prix n'existe pas.
- Les **escrocs de l'amitié** peuvent vous flatter et vous dire que vous êtes « beau/belle » ou « intéressant(e) », ou prétendre être très riche. Ils peuvent essayer de devenir votre ami, puis vous tromper ou vous amener à leur donner de l'argent ou à divulguer vos informations personnelles ou vos photos privées.
- Les **escrocs caritatifs** se font passer pour une organisation ou une personne qui collecte des dons pour aider une ou plusieurs personnes dans le besoin. Mais il s'avère qu'ils essaient simplement d'obtenir cet argent pour eux-mêmes.
- Les **escroqueries à l'emploi, aux prêts, aux investissements et à la crypto-monnaie** peuvent offrir un emploi formidable, un prêt bon marché ou un autre moyen de gagner rapidement de l'argent et demander un paiement pour accéder à l'opportunité, mais en réalité celle-ci n'existe pas.
- Le **hameçonnage (phishing)** consiste, pour un escroc, à tromper les gens en se faisant passer pour un véritable magasin, une banque ou une organisation, afin qu'ils communiquent des informations personnelles telles que leur nom, leur adresse, leurs coordonnées bancaires ou leurs mots de passe en ligne. Il peut ensuite utiliser ces informations pour se faire passer pour vous, afin d'escroquer de l'argent ou des informations à d'autres personnes.

Les escrocs créent aussi parfois de faux messages qui semblent provenir de Facebook. Facebook ne vous demandera jamais votre mot de passe dans un e-mail, ni ne vous enverra un mot de passe en pièce jointe. Pour en savoir plus, cliquez ici.

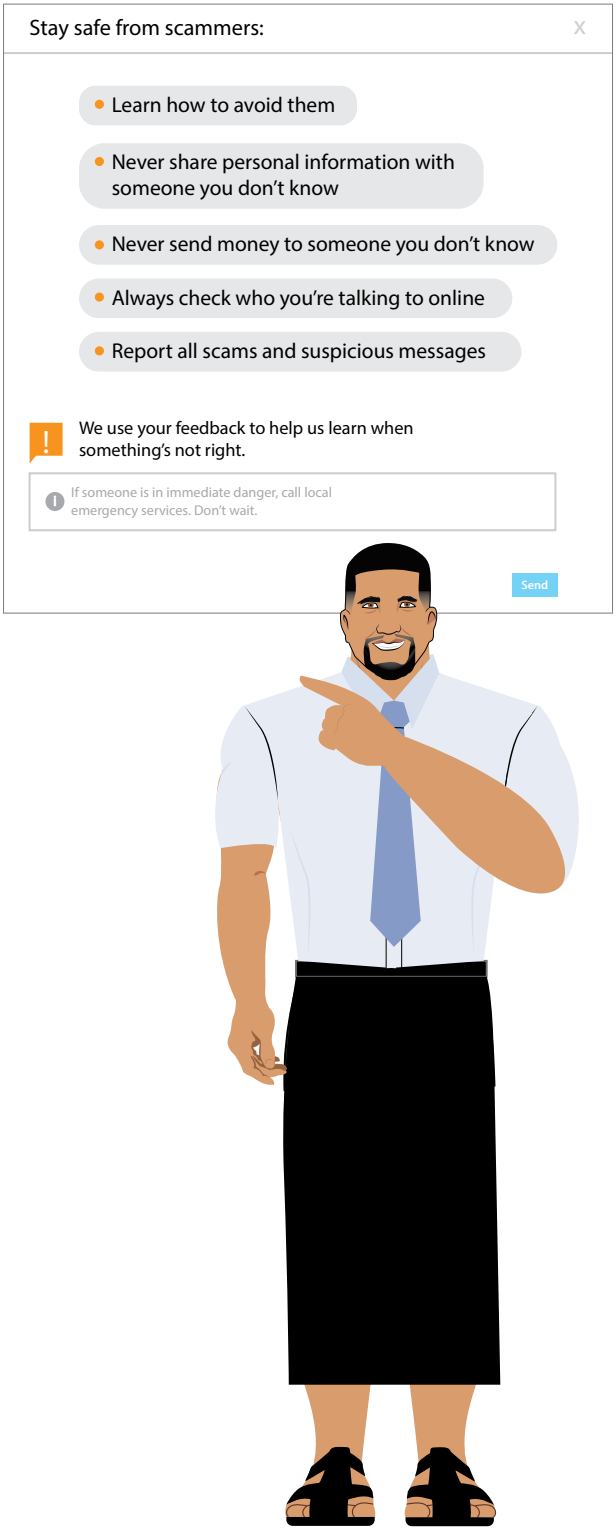
Comment repérer une escroquerie

Méfiez-vous des éléments suivants, ils peuvent être le signe qu'il s'agit d'une escroquerie :

- un message vous demandant de confirmer vos informations personnelles, telles que votre nom, votre adresse, votre date de naissance ou vos coordonnées bancaires ;
- une réclamation concernant un problème avec votre compte bancaire ou vos informations de paiement ;
- toute personne vous demandant de lui payer des frais ;
- messages comportant une menace ou un sentiment d'urgence ;
- messages comportant des fautes d'orthographe et de grammaire.

N'oubliez pas : si quelque chose semble trop beau pour être vrai… c'est probablement le cas.

Repérer et éviter les escroqueries en ligne cont.



Comment éviter les escroqueries

- Si vous avez des doutes sur un message que vous avez reçu, ne l'ouvrez pas et ne répondez pas à la personne.
- Soyez toujours prudent(e) si vous recevez un message de quelqu'un que vous ne connaissez pas.
- Ne versez jamais d'argent ou ne partagez jamais vos informations personnelles (ou celles de quelqu'un d'autre) avec une personne que vous ne connaissez pas. Les informations personnelles incluent le nom, l'âge, le numéro de téléphone, l'adresse électronique ou l'adresse du domicile, l'école ou une pièce d'identité avec photo (comme un passeport ou un permis de conduire)
- N'oubliez pas que les escrocs peuvent même se faire passer pour quelqu'un que vous connaissez, comme un ami ou un membre de votre famille. Si vous pensez que c'est le cas, vous pouvez contacter cette personne d'une autre manière pour vous assurer qu'il s'agit bien d'elle, par exemple en utilisant le numéro de téléphone que vous savez être le sien.
- Cherchez toujours à savoir à qui vous avez affaire. Visitez le site web officiel de l'organisation ou appelez son numéro de téléphone pour confirmer qu'elle est bien celle qu'elle prétend être.

Signalez immédiatement toute escroquerie ou tout message suspect. Découvrez comment signaler les escroqueries sur Facebook et Messenger, Instagram et WhatsApp.

Si vous pensez avoir été victime d'une escroquerie

- Si vous avez donné à un escroc vos informations de compte en ligne (identifiant, mot de passe, etc.), modifiez immédiatement votre mot de passe. Créez de nouveaux mots de passe forts et uniques.
- Si vous utilisez le même mot de passe pour plusieurs comptes ou sites web, modifiez-les tous.
- Si vous avez payé un escroc avec une carte bancaire, contactez immédiatement votre banque ou la société émettrice de votre carte bancaire. Signalez l'escroquerie et demandez quelles mesures vous pouvez prendre pour annuler les frais.

Si vous ou quelqu'un que vous connaissez êtes victime d'un acte criminel ou vous trouvez en danger immédiat, contactez les forces de l'ordre locales pour obtenir de l'aide.

Pour plus d'informations, consultez les Conseils pour éviter les escroqueries de Netsafe New Zealand.

Save the Children

#Jesuisnumérique