

Analyser des situations à risque

Trop beau pour être vrai? Attention au vol d'identité!

Les renseignements personnels peuvent être utilisés à des fins frauduleuses. Les protéger peut t'éviter des conséquences graves, comme le vol d'identité, la fraude financière ou l'accès non autorisé à tes comptes.



Signaux d'alerte

- Message urgent ou pressant
- Offre trop belle pour être vraie
- Informations vagues ou incomplètes
- Lien ou expéditeur inconnu
- Erreurs de langue ou présentation inhabituelle



Bons réflexes à adopter

- Vérifier la source (site officiel).
- Ne pas cliquer sur des liens suspects.
- Prendre le temps de réfléchir avant d'agir.
- En parler à une personne de confiance.
- Ne jamais transmettre de renseignements sensibles par message texte, courriel ou lien externe.



À vérifier avant de partager

- La source est-elle fiable et reconnue?
- La demande est-elle normale dans ce contexte?
- Les renseignements demandés sont-ils nécessaires?
- Attendais-tu cette demande?



Garde ça pour toi!

Ne partagez pas vos informations personnelles ou des données telles que les suivantes :

- NIP (numéro d'identification personnel)
- Code de sécurité (CVV)
- Numéro d'assurance sociale (NAS – utilisé pour l'emploi et les impôts)
- Codes de vérification (par exemple, codes reçus par texto ou application bancaire)
- Photo d'une pièce d'identité

Question clé

Cette demande est-elle sécuritaire et nécessaire?