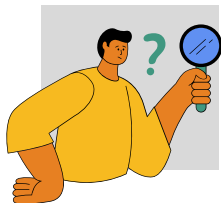


CYBER RÉFLEXES

DÉTECTER LA FRAUDE

1 MÉFIEZ-VOUS DES MESSAGES INATENDUS, SUSPECTS OU ALARMANTS

L'hameçonnage, aussi appelé *phishing*, est un stratagème de fraude visant à obtenir des informations personnelles pour diverses fins (vol d'identité, détournement de fonds, etc.). Les messages frauduleux sont non sollicités.



SIGNES À SURVEILLER

- Urgence : on vous presse d'agir ou vous menace.
- Profit : on vous informe que vous avez remporté un voyage/prix ou reçu un transfert d'argent dans votre compte.
- Problème : on vous signale un problème urgent à régler (exemple : avec votre compte bancaire ou la livraison d'un colis).

3 PRENEZ LE TEMPS D'EXAMINER CALMEMENT LE MESSAGE REÇU

Plusieurs indices sont typiques de messages frauduleux : un objet urgent, une adresse de provenance erronée, une salutation générique, un lien cliquable, une pièce jointe, des fautes d'orthographe ou de syntaxe, etc.

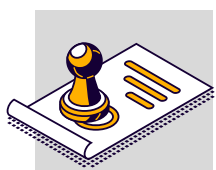


BONNES PRATIQUES

- Pensez avant de cliquer ; ne vous précipitez pas pour agir.
- Prenez le temps de réfléchir à la raison pour laquelle on vous contacte et si elle est véridique.
- En cas de doute, ne répondez-pas.

5 N'UTILISEZ PAS DE CONTENUS NON OFFICIELS

Les virus pouvant altérer vos appareils numériques ou vos comptes sont souvent présents dans les logiciels ou jeux piratés, les sites illégaux, etc.

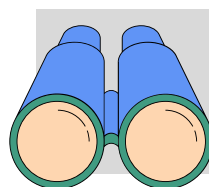


BONNES PRATIQUES

- Ne téléchargez pas de contenus illégaux ni de solutions non officielles.
- Installez uniquement des applications depuis les sites ou magasins officiels des éditeurs.

2 SOYEZ À L'AFFÛT PARTOUT

En se faisant souvent passer pour un organisme familier ou de confiance (banque, administration, etc.), les fraudeurs utilisent divers moyens pour entrer en contact avec vous.



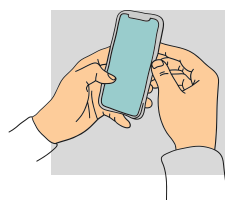
BONNES PRATIQUES

Restez à l'affût des indices de fraude sur tous les appareils numériques et systèmes que vous utilisez :

- **Messages (courriels, textos)** : on vous demande de cliquer sur un lien ou de donner vos renseignements personnels.
- **Appels** : on essaie de vous vendre un service ou vous demande de fournir des renseignements personnels.
- **Internet et réseaux sociaux** : on vous présente de fausses informations (conférences ou offres d'emploi).
- **Code QR** : on vous demande de scanner un code QR qui vous offrirait un rabais ou pour obtenir de l'information.

4 EFFECTUEZ LES MISES À JOUR RAPIDEMENT

Les appareils non maintenus à jour sont susceptibles de faire l'objet de failles de sécurité, rendant plus facilement exploitables les renseignements personnels qui s'y retrouvent.



BONNES PRATIQUES

- Faites les mises à jour de vos logiciels, applications et appareils dès qu'elles vous sont proposées.
- Activez les options de mises à jour automatiques lorsque possible.

Plus d'information sur
ulaval.ca/cybersecurite

Victime ou témoin d'une fraude?

Signalez-le rapidement au
Centre de cyberfédense ULaval.



UNIVERSITÉ
LAVAL