CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Hameçonnage par message texte : Se protéger contre les attaques par message texte

Avril 2026

ITSAP.00.103

L'hameçonnage par message texte est un type d'hameçonnage. Les auteurs de menace recourent au piratage psychologique pour envoyer des messages texte frauduleux conçus pour vous inciter à révéler de l'information sensible, comme des justificatifs d'ouverture de session ou des renseignements bancaires. Les messages texte utilisent un langage qui crée un sentiment d'urgence pour vous forcer à agir rapidement. Ces messages peuvent être liés à des maliciels ou à de faux sites Web, ce qui permet aux auteurs de menace de voler vos données, votre argent ou votre identité.

La présente publication a été rédigée en collaboration avec la Gendarmerie royale du Canada afin de sensibiliser les gens au repérage, au signalement et à la réduction des arnaques d'hameçonnage par message texte.

Comment les auteurs de menace exploitent l'hameçon-

Les techniques modernes d'hameçonnage par message texte permettent aux auteurs de menace d'usurper le numéro de téléphone de l'expéditeur, ce qui fait en sorte que le message semble provenir directement d'une organisation bien connue à laquelle vous faites confiance. Par exemple, si des auteurs de menace usurpent le code abrégé légitime de votre banque, les messages frauduleux apparaîtront dans le même fil de clavardage où se trouvent toutes les communications légitimes que vous auriez eues avec votre banque par le passé. La poursuite de la conversation fait qu'il est très difficile de distinguer les messages frauduleux des messages valides.

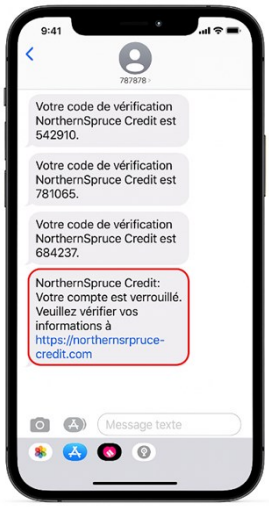
Comment reconnaître un message d'hameçonnage par

Bien que le nom et le numéro de l'expéditeur d'un message d'hameçonnage par message texte puissent sembler légitimes, voici des signes précurseurs dont vous devez vous méfier :

- des messages urgents concernant des comptes « bloqués » ou « compromis »;
- des liens suspects créés au moyen de raccourcisseurs d'URL ou d'adresses Web légèrement modifiées;
- des demandes de renseignements sensibles, comme des mots de passe, des numéros d'identification personnels ou des numéros d'assurance sociale.

Ce sont tous des renseignements que les organisations légitimes ne solliciteraient pas par message texte.

Figure 1: Example of a smishing message



SÉRIE SENSIBILISATION

PS74-33/2026F-PDF

ISBN 978-0-660-99748-3

Se protéger contre l'hameçonnage par message texte

Pour vous protéger contre les attaques par hameçonnage par message texte, suivez les stratégies d'atténuation recommandées ci-dessous :

- **Ne pas cliquer sur des liens :** Ne cliquez pas sur des liens que vous recevez par message texte. Si vous recevez un message urgent ou un message contenant un lien suspect ou inhabituel, réfléchissez avant de réagir. Les fraudeurs misent sur des réactions impulsives. Allez au portail en ligne officiel de l'organisation à l'aide de votre navigateur ou de votre application mobile officielle.
- **Vérifier la demande de façon indépendante :** Si un message s'affiche dans un fil de discussion légitime (p. ex. celui de votre banque), composez le numéro indiqué au verso de votre carte de débit ou de crédit pour vérifier la demande. Ne composez pas le numéro indiqué dans le message texte.
- **Signaler les messages texte indésirables :** Transférez le message texte suspect au numéro 7726 (SPAM) ou utilisez la fonction de signalement des messages texte indésirables de l'application de messagerie. Vous pouvez également signaler les messages texte indésirables au Centre antifraude du Canada. Ainsi, les organisations concernées seront avisées de lancer une enquête et de prendre les mesures pertinentes.
- **Activation de l'authentification multifacteur (AMF) :** Ensure MFA is enabled on your accounts to prevent unauthorized access even if credentials are stolen. Whenever possible, choose MFA options that do not rely on SMS like an authenticator app, or options that are phishing-resistant such as passkeys, or hardware tokens.
- **Désactiver la technologie 2G :** ISi votre téléphone le permet, désactivez la technologie 2G dans les paramètres. Ce faisant, vous pouvez empêcher la connexion de votre téléphone à une fausse station de base exploitée par un auteur de menace.
- **Demeurer à jour :** Assurez-vous que le logiciel de votre appareil est à jour et activez la protection contre les messages texte indésirables.
- **Supprimer les messages suspects :** Si l'expéditeur suspect est un nouveau numéro, bloquez-le. Supprimez les messages suspects pour éviter de cliquer accidentellement sur le lien.

Pour en savoir plus

- Hameçonnage par message texte : Une introduction
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Hameçonnage : Ne vous laissez pas prendre
- Les 7 signaux d'alarme de l'hameçonnage
- Fiche d'information : Hameçonnage
- Trois types fréquents d'hameçonnage
- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)
- Signaler les messages textes indésirables au numéro 7726

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.