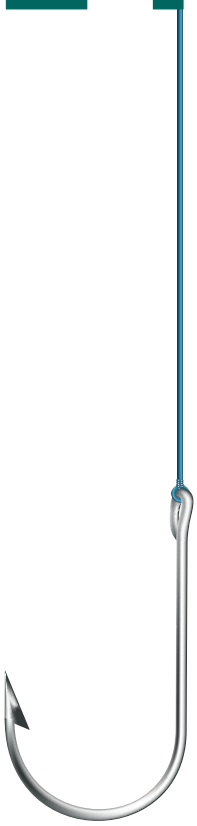
L'HAMEÇONNAGE



Apprenez-en plus sur cette tactique utilisée par les fraudeurs pour voler des renseignements confidentiels.

QU'EST-CE QUE L'HAMEÇONNAGE?

L'hameçonnage est un stratagème de fraude. Il s'agit d'une stratégie qui vise à s'approprier de façon illégitime l'identité d'une organisation lors de l'envoi de courriels ou de textos ou de redirection vers un faux site Internet pour vous inciter à révéler des informations personnelles et corporatives confidentielles. Les cybercriminels utilisent des techniques de manipulation pour voler des données, infecter des ordinateurs et infiltrer les réseaux d'entreprises et d'organisations.

Avec ces messages frauduleux, les cybercriminels cherchent à vous faire cliquer sur des liens, des images ou des fichiers. C'est une technique de manipulation utilisée pour voler vos informations ou d'installer des logiciels malveillants sur votre appareil sans que vous le sachiez.

COMMENT DÉTECTER L'HAMEÇONNAGE?

Les messages d'hameçonnage sont non sollicités. Les fraudeurs misent sur des situations ou sur des urgences pour vous pousser à réagir rapidement puis à partager vos renseignements. Puisqu'on se croit sous pression, c'est dans ces moments d'urgence que l'on est parfois le plus vulnérable.

QUELQUES EXEMPLES DE SITUATIONS D'HAMEÇONNAGE

- URGENCE
On vous presse de mettre à jour vos coordonnées

- PROFIT
On vous fait miroiter un profit, on vous informe que vous avez remporté un prix ou que vous avez reçu un transfert d'argent dans votre compte.

- PROBLÈME
On vous signale un problème urgent à régler avec votre compte bancaire, votre système d'exploitation ou encore la livraison d'un colis.

RECONNAÎTRE UN SITE FRAUDULEUX

Pour vous piéger, les fraudeurs vous redirigent vers de faux sites qui ressemblent à s'y méprendre à un site légitime. Certains indices peuvent vous aider à les repérer et à éviter de tomber dans le panneau.

- Le faux site est mal conçu et renvoie une image peu professionnelle
- L'adresse est modifiée de façon sournoise (.org alors qu'elle devrait être .com)
- Le logo n'est pas de la même qualité qu'à l'habitude, il n'est pas exactement le même
- Les textes comportent des fautes d'orthographe
- Les liens sont brisés
- Les coordonnées de l'entreprise sont difficiles à trouver
- Le site vous invite à entrer vos renseignements alors qu'en temps normal vous n'avez pas à le faire

VOUS AVEZ UN DOUTE?

QUE FAIRE SI VOUS SOUPÇONNEZ UNE TENTATIVE D'HAMEÇONNAGE?

Prenez un temps d'arrêt et examinez le message que vous avez reçu. Dans l'immédiat, ne cliquez sur aucun lien et n'ouvrez aucune image ou pièce jointe. Ne répondez pas à l'expéditeur pour ne pas confirmer la validité de votre adresse courriel.

CE QUI PEUT ÊTRE RAPIDEMENT VÉRIFIÉ

L'ADRESSE COURRIEL

- Assurez-vous que l'adresse courriel de l'expéditeur vous semble connue et légitime.
- Validez l'adresse officielle en portant une attention particulière après le ***a*** commercial (@).
- Vérifiez s'il s'agit d'une adresse courriel personnelle ou professionnelle.

LE LIEN

- Inspectez le lien pour définir s'il mène vraiment au site d'une organisation légitime ou connue. Prêtez attention aux détails : les fraudeurs ne changent parfois qu'une seule lettre pour mieux vous duper.*
  - ⇨ Sur un ordinateur, survolez le lien avec votre curseur sans cliquer dessus, l'adresse apparaitra.
  - ⇨ Sur un appareil mobile, appuyez quelques secondes sur le lien, jusqu'à ce qu'une fenêtre contextuelle vous affiche l'adresse au long.

**Sur le réseau du CSSDA, cette pratique n'est pas nécessaire puisque des vérifications de sécurité sont faites au préalable.*

LE CONTENU

Demandez-vous si les raisons pour lesquelles on vous pousse à agir rapidement sont plausibles et justifiées. Pour quelle raison vous sollicite-t-on à répondre si rapidement ? Est-ce crédible que l'on vous presse de la sorte ? Avez-vous habituellement à entrer ces données?

EN CAS DE DOUTE

En cas de doute, ne transférez pas le courriel et n'ouvrez pas de pièce jointe.

Signalez l'incident au Service de technologies de l'information (STI) par une **Demande de service TI** sous la section **Sécurité informatique / déclaration d'événement**.

Un suivi vous sera rapidement assuré par l'équipe TI pour vous transmettre les instructions à suivre.

Centre
de services scolaire
des Affluents
Québec