Centre
de services scolaire
du Fleuve-et-des-Lacs
Québec

DIRECTIVE ENCADRANT LA DÉCLARATION DES COURRIELS D'HAMEÇONNAGE

SERVICE DES RESSOURCES INFORMATIONNELLES
RÈGLEMENTS, DIRECTIVES, POLITIQUES ET PROCÉDURES

1er mars 2023

Table des matières

1. PRÉAMBULE

L'utilisation des ressources informatiques de façon sécuritaire est une priorité organisationnelle et les organismes publics sont tenus de respecter les directives gouvernementales.

2. OBJECTIFS

La présente directive vise à encadrer la démarche à suivre afin d'identifier une attaque informatique de type hameçonnage et de gérer sa déclaration.

3. DÉFINITIONS

3.1 Hameçonnage

Consiste à envoyer des courriels de masse qui semblent provenir d'un collègue, d'un ami ou d'une institution connue, mais qui contiennent une pièce jointe infectée ou un lien malveillant. Les courriels sont rédigés de manière à inciter les destinataires à ouvrir une pièce jointe ou à cliquer sur un lien pour permettre aux auteurs de menaces d'obtenir des justificatifs d'identité personnelle ou d'accéder à un système informatique et à son contenu.

3.2 Incident de type hameçonnage

Toute tentative frauduleuse exploitant un composant du système d'information (messagerie électronique, téléphone, plateforme de partage telle qu'Office 365 et DropBox, etc.) et demandant à un utilisateur de cliquer sur un lien, de télécharger une pièce jointe ou de divulguer une information confidentielle.

3.3 Tactiques d'ingénierie sociale

L'ingénierie sociale est une technique de manipulation utilisée par les pirates informatiques pour inciter les gens à partager des informations confidentielles.

Elle mise sur la nature de l'être humain à faire confiance pour voler des informations personnelles et corporatives qui peuvent ensuite être utilisées pour commettre d'autres cybercrimes.

Par exemple, un pirate informatique peut utiliser l'hameçonnage pour convaincre un employé de divulguer des mots de passe de l'entreprise. Ceux-ci sont ensuite utilisés pour accéder aux réseaux de l'entreprise, voler des données et installer un logiciel malicieux.

Pour que le pirate informatique gagne la partie, il suffit d'un courriel, d'un appel téléphonique ou d'un message texte semblant provenir d'un collègue, d'un ami ou d'une institution connue. Dans son message, le pirate informatique peut utiliser un ton pressant pour convaincre l'utilisateur de mettre à jour ses informations bancaires, ou préciser que pour réclamer son prix, il doit fournir ses informations de carte de crédit.

4. PROCESSUS D'ÉVALUATION

La présente démarche vise à orienter l'utilisateur face aux menaces informatiques de type hameçonnage. Comme il s'agit d'une méthode régulièrement utilisée par les pirates informatiques, les utilisateurs doivent porter une attention particulière aux courriels reçus dans leur boite de courriel institutionnel. Chaque utilisateur doit être en mesure d'évaluer la sécurité des courriels qu'il reçoit, afin de déterminer quand il doit signaler un incident de type hameçonnage au Service des ressources informationnelles (SRI).

Les pirates informatiques qui envoient des courriels menaçants ont recourt à des tactiques d'ingénierie sociale et leurs courriels revêtent souvent un caractère urgent. À titre d'exemple, peut constituer un incident de type hameçonnage la réception de courriels tel que l'on retrouve à l'annexe I.

Évitez absolument de cliquer sur un hyperlien, d'ouvrir une pièce jointe ou de transmettre des informations si vous ne connaissez pas l'expéditeur du courriel, ou si l'adresse courriel de votre interlocuteur vous paraît étrange. En cas de doute, n'hésitez pas à soumettre le courriel pour analyse à l'équipe de soutien technique à l'adresse courriel : Cybersecurite@cssfl.gouv.qc.ca

4.1. Détection d'un incident de type hameçonnage

4.1.1. Si l'adresse courriel de l'expéditeur est inconnue ou illégitime

1. Vérifiez la présence d'une pièce jointe ou d'un lien internet intégré au courriel ;

2. N'ouvrez pas la pièce jointe et ne cliquez sur aucun lien contenu dans celui-ci ;

3. Vérifier si le lien et l'adresse de l'expéditeur sont cohérents
   - En prenant soin de ne pas cliquer, vous pouvez placer le curseur de votre souris au-dessus du lien pour vérifier l'adresse du lien internet.
   - Vous pouvez faire la même chose pour le nom de l'expéditeur et vérifier si l'adresse de l'expéditeur correspond à l'organisation que celui-ci prétend représenter.

4. Si, après avoir vérifié et appliqué les points 1 à 3 ci-dessus, vous croyez avoir reçu un courriel d'hameçonnage, vous devez signaler un incident de type hameçonnage conformément à l'article 4.2 de la présente directive.

4.1.2. Si l'expéditeur est un collègue, un ami ou une institution connue

1. Vous devez vérifier l'objet, le contexte et le style d'écriture ;

2. Si vous remarquez des choses inhabituelles ou non sollicitées, vous devez confirmer l'identité de l'expéditeur par un autre canal (appel téléphonique, SMS, Teams, Zoom) ;

3. Si la personne concernée n'a pas confirmé l'envoi de ce courriel, vous devez signaler un incident de type hameçonnage conformément à l'article 4.2 de la présente directive.

4.2. Déclaration d'un incident de type hameçonnage

1. Vous devez déclarer un incident de type hameçonnage en transférant le courriel menaçant à l'adresse suivante : Cybersecurite@cssfl.gouv.qc.ca

2. Vous devez conserver le courriel menaçant le temps que le SRI procède à son analyse, puisqu'il pourrait s'agir d'un courriel illégitime et que des informations essentielles à l'enquête s'y retrouvent.

4. RESPONSABILITÉS DU SRI

Une fois qu'un incident de type hameçonnage est signalé par un utilisateur, le SRI doit mener une évaluation afin de vérifier qu'il ne s'agit pas d'un faux positif, et ce, avant de lancer le processus de réponse aux incidents et la démarche de déclaration d'incidents auprès du Centre opérationnel de cyberdéfense du Ministère de l'Éducation (COCD).

Le SRI procédera à l'analyse dans les meilleurs délais et vous tiendra informé par l'entremise de son système de gestion des requêtes informatiques.

5. DIVULGATION AU COCD

L'analyse permettra de déterminer l'ampleur de l'attaque et déterminera le niveau d'escalade à apporter. Le coordonnateur organisationnel des mesures en sécurité de l'information (COMSI) et le chef de la sécurité de l'information organisationnelle (CSIO) du CSSFL seront informés.

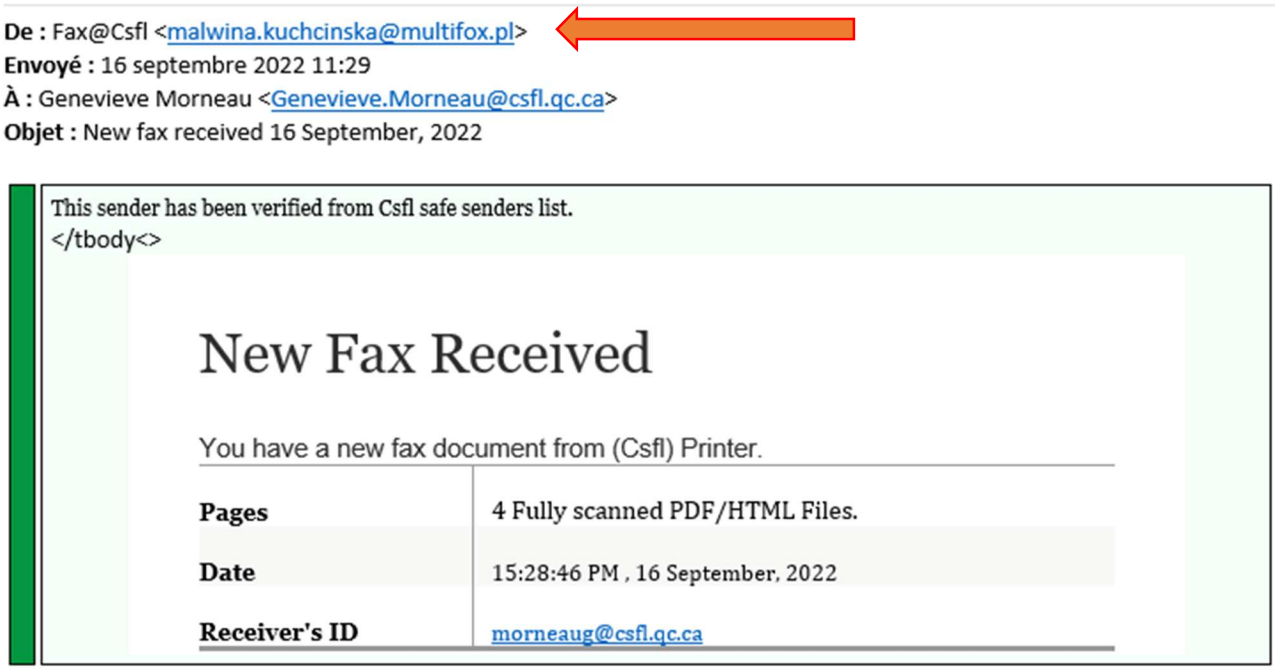
En fonction des résultats de l'analyse, le COMSI déterminera si une déclaration au COCD est requise.

6. MISE EN ŒUVRE ET MODIFICATION

En vertu de la *Politique relative à la gestion et à la sécurité des actifs informationnelles*, le Directeur du SRI détient les fonctions de CSIO. Se faisant, il s'assure de la mise en œuvre de la présente directive.

ANNEXE 1 : EXEMPLES DE COURRIELS D'HAMEÇONNAGE

Exemple 1



De : Fax@Csfl <malwina.kuchcinska@multifox.pl>
Envoyé : 16 septembre 2022 11:29
À : Genevieve Morneau <Genevieve.Morneau@csfl.qc.ca>
Objet : New fax received 16 September, 2022

This sender has been verified from Csfl safe senders list.
</tbody<>

New Fax Received

You have a new fax document from (Csfl) Printer.

Pages	4 Fully scanned PDF/HTML Files.
Date	15:28:46 PM , 16 September, 2022
Receiver's ID	morneaug@csfl.qc.ca

Vérifier l'adresse de l'expéditeur du courriel, cette adresse @multifox.pl correspond à la Pologne.

Exemple 2

Netflix Inc.

N noreply@companiesdiscounts.com
À Pascal Lévesque

Répondre | Répondre à tous | Transférer | ...
jeu. 2022-11-17 12:54

NETFLIX

Veuillez mettre à jour votre mode de paiement

Bonjour,

Nous éprouvons des difficultés à autoriser votre carte de crédit. Veuillez visiter le www.netflix.com/youraccountpayment Link pour entrer de nouveau vos renseignements de paiement ou utiliser un autre mode de paiement. Lorsque vous aurez terminé, nous tenterons de vérifier de nouveau votre compte. Si la vérification échoue de nouveau, nous vous recommandons de communiquer avec l'émetteur de votre carte de crédit.

Nous serons heureux de vous aider si vous avez des questions. Il vous suffit de nous appeler, en tout temps, au 1 800 096 6380.

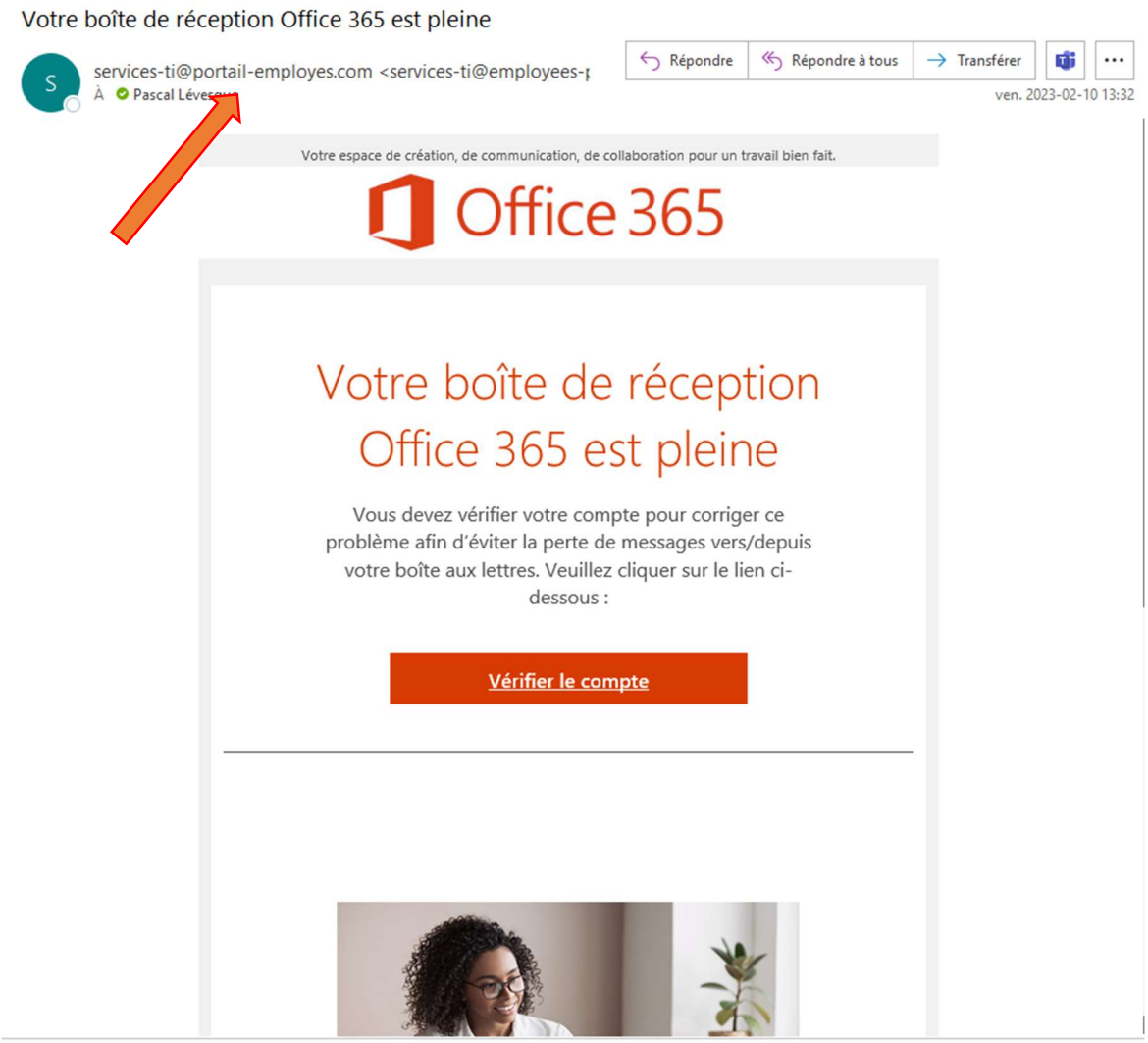
-L'équipe Netflix

Des questions? Composez le **1 800 096 6380**

Ce courriel relatif à votre compte vous a été envoyé dans le cadre de votre abonnement à Netflix. Pour changer vos préférences de courriel, vous pouvez visiter en tout temps la page Préférences de courriel de votre compte. Veuillez ne pas répondre à ce courriel. Nous ne sommes pas en mesure de répondre aux courriels envoyés à cette adresse. Si vous avez besoin d'aide ou souhaitez communiquer avec nous, veuillez visiter notre centre d'aide à help.netflix.com.

Encore une fois l'expéditeur du courriel est : @companiesdiscounts.com cette adresse n'est pas celle de Netflix. Le numéro de téléphone est cliquable. Le lien qui est dans le courriel ne pointe pas sur netflix.com

Exemple 3



Vous devez toujours vous méfier des adresses courriel qui vous envoient un message.

Lorsque vous recevez un message de Microsoft, vérifiez pour que ce soit bien @microsoft.com qui vous envoie un courriel. Dans notre cas : @portail-employes.com n'est pas une adresse Microsoft.

Autre point important, depuis notre migration vers Office 365 les boîtes courriels fournies par Microsoft ont un espace de stockage de 1000 go. Il très peu probable que votre limite de stockage soit pleine.