Consignes pour l’usage des liens cliquables

Centre opérationnel de cyberdéfense

COCD

Votre gouvernement

Québec

CONTEXTE

Faisant suite à l'envoi de la lettre du 16 janvier 2024 concernant l'utilisation de liens cliquables, un comité inter-établissement de santé fut mis sur pied par Yvan Fournier, responsable opérationnel de la cyberdéfense (ROCD) du réseau de la santé.

L'objectif de ce comité est de répondre aux différentes questions recueillies sur la mise en place de cette lettre, comment y répondre de manière adéquate, et de proposer des solutions de contournement à court et moyen termes. Ce document, qui se veut évolutif dans le temps, est une première référence pour les gens du réseau de la santé et des services sociaux (RSSS).

Référence :

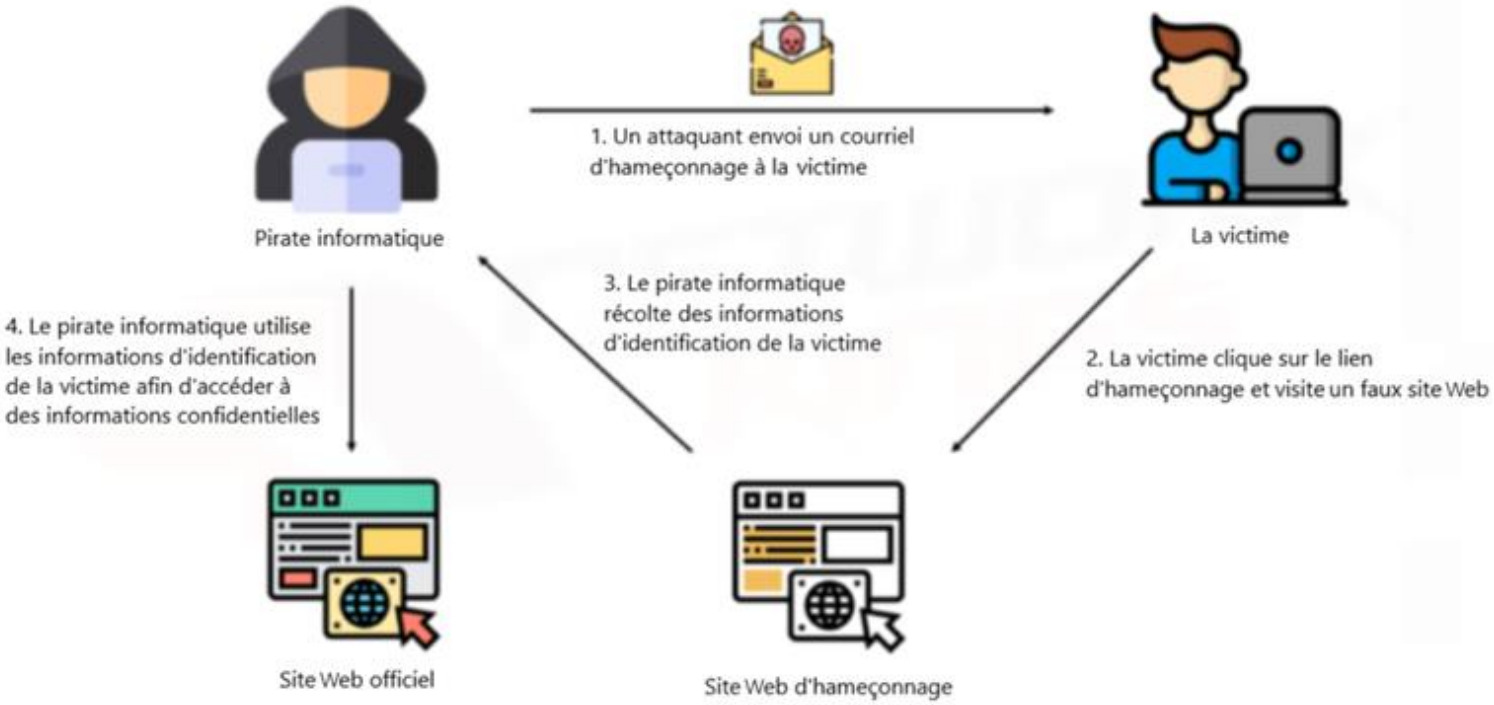
MSSS-EXI-009-Exigence-encadrant-les-communications-numeriques-avec-les-citoyens

POURQUOI CETTE DIRECTIVE EST-ELLE IMPORTANTE?

Saviez-vous qu'un attaquant peut falsifier un lien URL et voler des informations personnelles ou confidentielles d'une victime?

En truquant le lien URL, la victime pense cliquer sur un lien sécuritaire et officiel alors que ce n'est pas le cas.

POURQUOI CETTE DIRECTIVE EST-ELLE IMPORTANTE?



POURQUOI CETTE DIRECTIVE EST-ELLE IMPORTANTE?

Les attaques par hameçonnage sont l'un des vecteurs très utilisés qui sont de plus en plus sophistiquées et dont les mesures d'identification sont de plus en plus difficiles.

Exemple : gouvernement vs gouvernernent
La lettre m est une combinaison de la lettre r + n pour faire rn.

L'usage des outils comme l'intelligence artificielle augmentera le nombre de courriels d'hameçonnage à devenir plus réaliste au fil des années.

Il est possible qu'un pirate informatique utilise la technique d'attaque dite « l'homme du milieu » (MITM). Ceci permet d'intercepter un courriel et de :

- Falsifier un lien URL puis le retourner au destinataire sans laisser de trace afin de tromper le destinataire;
- Visualiser des données entre deux communications officielles, ce qui peut amener une violation de la vie privée.

RISQUES

En résumé, les risques sont les suivants :

- Atteinte à la vie privée;
- Vol de données de nature personnelles ou confidentielles;
- Vol d’identifiants de connexion amenant à une violation d’accès;
- Redirection vers un site Web malveillant pouvant installer des logiciels malveillants (malwares) sur un ordinateur.

PRINCIPES DE BASE

1. Le lien cliquable ne peut être utilisé dans le cadre d'une communication non sollicitée par le récepteur.
2. Le lien cliquable peut être dangereux même s'il ne renvoie pas à un site qui récolte des données personnelles confidentielles.
3. La possibilité de créer des liens frauduleux existe toujours, même s'il s'agit d'un lien d'apparence sécuritaire (https).

ACTIONS À ÉVITER

- Envoyer des liens cliquables **à l'externe** (citoyens, journalistes, partenaires et autres), même vers des sites reconnus comme Québec.ca
- Envoyer **un lien cliquable *par texto* (SMS)** vers une entité externe (citoyens, journalistes, partenaires et autres)
- Mettre un lien **sans le rendre cliquable**
- Envoyer un **document en pièce jointe incluant des liens cliquables**
- Utiliser une **application de marketing par courriel sécurisée** pour envoyer des liens cliquables
- Envoyer un lien cliquable **dans une infolettre envoyée par texto (SMS) ou par courriel** vers une entité externe (citoyens, journalistes, partenaires et autres)
- Inclure un lien **dans une signature courriel**

USAGE AUTORISÉ DES LIENS CLIQUABLES ET EXCEPTIONS

- ✓ Envoyer un lien cliquable à **l'interne** (dans le réseau de la Santé et des Services sociaux)
- ✓ Envoyer un lien cliquable menant à une rencontre **Teams** à l'externe lorsque la personne sait qu'elle participera à un appel
- ✓ Envoyer un lien cliquable *par courriel* dans le contexte d'une relation de soins en **télésanté** (incluant les rencontres Teams et les ressources informationnelles d'un site Web)
- ✓ Envoyer un lien cliquable en réponse à une **action liée à l'authentification spécifiquement initiée par l'utilisateur**, comme lors d'un processus de réinitialisation de mot de passe, pourvu que la validité du lien soit temporairement limitée
- ✓ Envoyer un lien cliquable par courriel **lors d'une interaction directe** avec un intervenant, que ce soit en visioconférence ou en personne, à condition que le citoyen en soit informé au cours de cette interaction et que la validité du lien soit limitée dans le temps

SOLUTIONS PROPOSÉES

Envoi d’un lien dans un courriel

- Inclure des images dans votre courriel pour faciliter vos explications
- Modifier votre site public pour créer une section qui liste l'ensemble des liens davantage utilisés
- Inciter les gens à utiliser la fonction de recherche de votre site et leur indiquer quel mot-clé rechercher pour trouver le contenu qui les intéresse
- Rediriger vers des sites connus en mentionnant le nom du site sans fournir l’adresse URL directement

SOLUTIONS PROPOSÉES

Sondage

Pour ce qui réfère aux liens vers des sondages de satisfaction de votre établissement, nous proposons de mettre en évidence une **section « *Sondage* » sur la page d'accueil** du site public de votre établissement.

Dans les courriels ou textos (SMS) envoyés à une entité externe, vous pouvez diriger vers la section en question en indiquant à l'entité externe de se rendre sur le site officiel de l'établissement sans inclure le lien cliquable vers ce dernier.

SOLUTIONS PROPOSÉES

Échange de documents

1. Si vous devez partager des documents, des informations sensibles ou des ressources avec une entité externe comme une clinique, **un compte Microsoft de type invité peut être créé pour votre établissement**.

   Ceci permettra d'accéder au tenant Microsoft 365 et d'utiliser des applications comme Teams, assurant ainsi la sécurisation des informations transférées.

   Attention : Évidemment, des coûts de licence sont à considérer ici.

2. Vous pouvez aussi utiliser des **plateformes de transfert de fichiers sécurisés**, tant que celles-ci respectent les bonnes pratiques de sécurité et les 15 mesures obligatoires de sécurité.