Questions pour la discussion

Guide de réunion

Novembre 2025

Ingénierie sociale et hameçonnage

cyber eco

Qu'est-ce que l'ingénierie sociale?

Les pratiques d'ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou organisations pour obtenir quelque chose frauduleusement.

– Paul Wilson et A.T. Chandler, Social Engineering The Art of Human Hacking

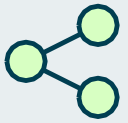
- En exploitant la confiance, l'urgence, la peur ou même une promesse de gain, le fraudeur a pour objectif d'obtenir des informations sensibles ou d'inciter la victime à poser un geste impulsif.
- L'ingénierie sociale peut se vivre sous différentes formes (appel téléphonique, courriel, en personne).

Pour qui peuvent-ils se faire passer?

- Membre de famille ou ancien camarade
- Dirigeant, collègue, fournisseur ou client
- Représentant du gouvernement ou de la police

Connaissez-vous les méthodes d'attaque par ingénierie sociale?

Téléphone



Réseaux sociaux

Courriels et textos

Accès physique

Applications web

Qu'est-ce que l'hameçonnage ou phishing?

L'hameçonnage est un stratagème qui consiste à envoyer massivement des courriels ou des messages textes (SMS) dans le but de réaliser une fraude en trompant la vigilance de l'utilisateur.

C'est une forme d'ingénierie sociale qui permet d'ouvrir la première porte du réseau de l'entreprise.

INCITE

le destinataire à cliquer sur un lien ou à ouvrir une pièce jointe qui permettra au fraudeur :

- de voler des informations personnelles
- d'installer un logiciel malveillant sur l'appareil

Comment reconnaître l'hameçonnage?

Avant de cliquer, on **valide**

1

Le courriel ou message texte est-il attendu et sollicité?

2

La demande ou situation m'incite-t-elle à réagir rapidement ou avec un sentiment d'urgence?

3

L'adresse courriel de l'expéditeur me semble-t-elle connue et légitime? Qu'y a-t-il après l'arobas? **@microsotf**?

Comment reconnaître l'hameçonnage?

Avant de cliquer, on **valide**

4

Qu'est-ce qui apparait en déplaçant le curseur sur le lien hypertexte (sans cliquer)?

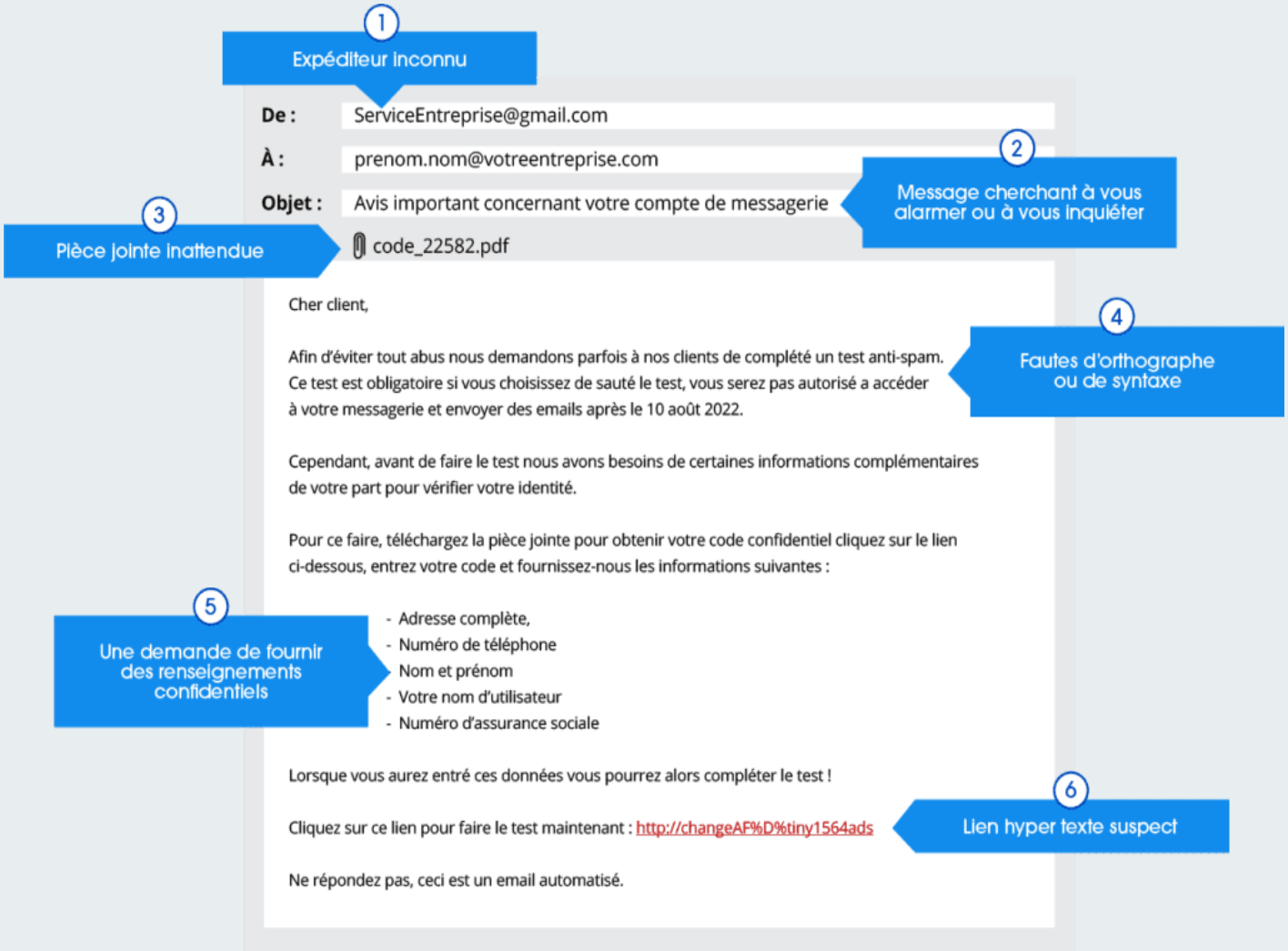
5

Le courriel est-il pertinent et vraisemblable?

6

Est-ce que je me laisse distraire par la curiosité, l'identité visuelle et logo que je connais bien?

Sauriez-vous reconnaître une tentative d'hameçonnage?



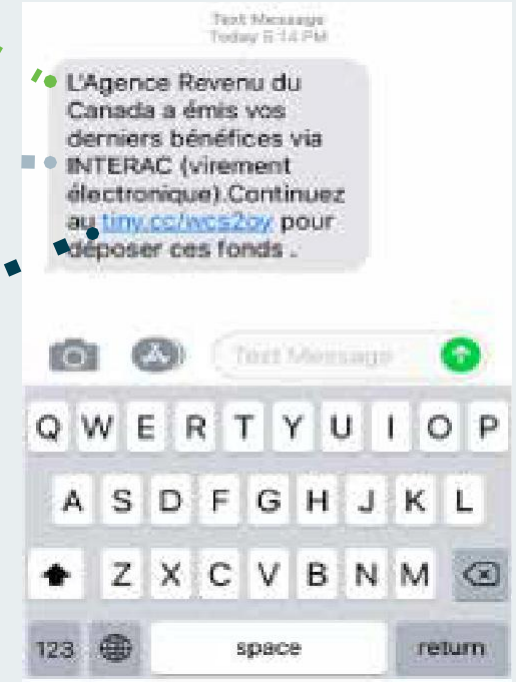
Sauriez-vous reconnaître une attaque recourant à l'ingénierie sociale?

Les cybercriminels utilisent les messages textes pour personnifier une institution financière, une entreprise de téléphonie, un gouvernement, Interac ou toute autre institution connue. L'objectif? Soutirer des renseignements personnels en vous incitant à cliquer sur un lien (comme l'illustre la photo) ou en installant un logiciel malicieux.

Expéditeur qui semble de confiance

Instructions de paiement inhabituelles

Invitation à cliquer sur un lien



Comment prévenir les tentatives d'hameçonnage et d'ingénierie sociale?

- Limiter les informations publiées sur vos réseaux sociaux et votre site Internet
- Limiter l'utilisation de l'adresse courriel liée à l'entreprise à des fins professionnelles seulement
- Être vigilant à la réception d'appels et de courriels non sollicités
- Recourir à un logiciel antivirus et à un pare-feu pour bloquer les menaces, et vous assurer de les mettre à jour régulièrement

Que faire avec un message texte frauduleux?

Vous pouvez signaler un message texte suspect (hameçonnage ou fraude) en **le transférant au numéro 7726** (« **SPAM** » sur le clavier de votre téléphone)

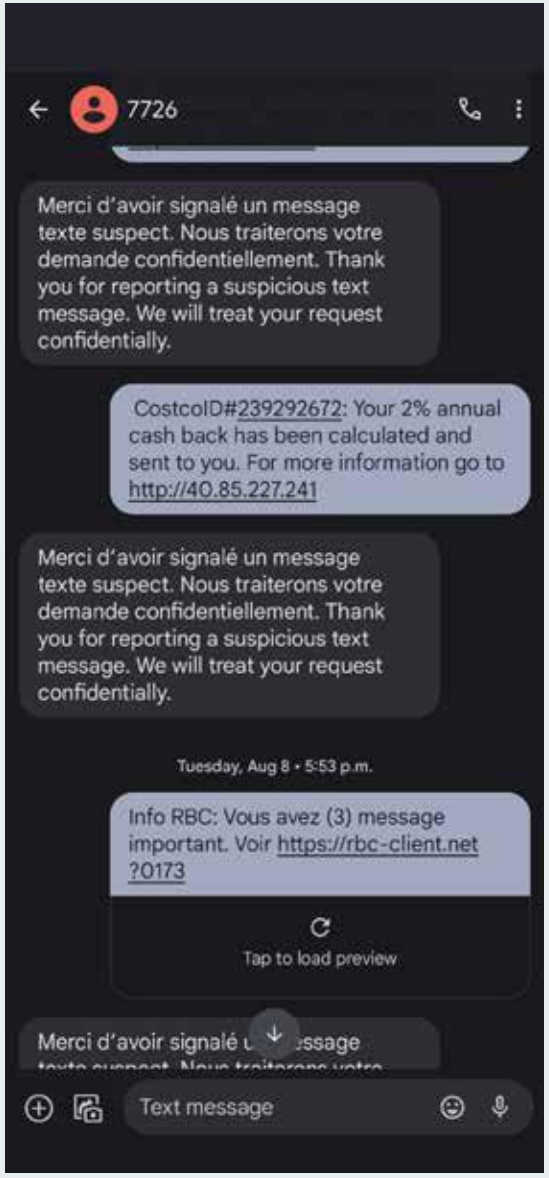
COMMENT FAIRE?

1. Sélectionnez le texto suspect
2. Choisissez « Transférer »
3. Entrez « 7726 » comme destinataire
4. Envoyez le message

C'est le moyen officiel et rapide de signaler ces tentatives d'hameçonnage au Canada.

L'OBJECTIF?

Aider votre fournisseur de téléphonie (Bell, Rogers, Telus, etc.) à identifier et À bloquer les numéros qui envoient des messages frauduleux.



Que faire si on pense avoir été victime d'hameçonnage?

1. Changer immédiatement ses mots de passe
2. Prévenir votre service TI ou votre fournisseur de messagerie
3. Ne **pas** transférer ni répondre au message frauduleux
4. Surveiller ses comptes et signaler l'incident aux autorités

En conclusion

Faites preuve de vigilance!

Une attaque d' hameçonnage peut s'avérer désastreuse sur le plan financier et sur l'image d'une entreprise.

Pour protéger la nôtre contre l'hameçonnage et l'ingénierie sociale, votre **vigilance** et votre **bon jugement** peuvent faire toute la différence!

Références

- Hameçonnage : reconnaître les fausses communications | Banque Nationale
- Détecter et signaler une fraude | Desjardins

Licence et Avertissement

Sujet au respect des termes et conditions de cette licence, Cybereco vous octroie le droit gratuit et non-exclusif d'utiliser et de reproduire ce matériel à des fins internes ainsi que de le partager selon les mêmes termes et conditions. Le matériel ne peut être modifié et la marque de Cybereco et les termes et conditions de cette licence doivent y demeurer apposés tels quels.

Cette licence ne vous permet pas de revendiquer quelque droit de propriété intellectuelle dans le matériel, de le vendre ou d'utiliser toute marque de commerce qui y est contenue séparément sans l'autorisation de son propriétaire.

Les renseignements contenus dans ce matériel sont d'ordre général seulement et ne constituent pas des conseils ou de services professionnels. Avant de prendre une décision ou de prendre des mesures qui pourraient avoir une incidence sur vos finances ou vos activités, vous devriez consulter un conseiller professionnel qualifié.

Ce matériel est mis à votre disposition « tel quel » et sans aucune garantie. Sans limiter la portée de ce qui précède, Cybereco ne garantit pas que le matériel puisse être utilisé conformément à l'usage auquel il est destiné, qu'il ne contient aucune erreur, ni aucun virus ou programme malveillant, ni qu'il répond à des critères précis en matière de sécurité, de rendement ou de qualité.

Toute garantie implicite de qualité marchande, de caractère approprié à une fin donnée, de titre et à l'absence de violation de droits de propriété intellectuelle, à la compatibilité, à la sécurité et à l'exactitude est expressément rejetée.

L'utilisation de ce matériel est à vos propres risques, et c'est à vous d'assumer la pleine responsabilité et de toute perte résultant de cette utilisation, y compris, sans s'y restreindre, toute interruption de services ou perte de données. Nous n'assumerons aucune responsabilité à l'égard de dommages-intérêts directs, indirects, spéciaux, accessoires, consécutifs ou punitifs, ni d'aucun autre dommage quel qu'il soit, que ce soit dans une action en justice recherchant une responsabilité contractuelle, juridique ou délictuelle (y compris, sans s'y restreindre, la négligence) ou autrement, relativement à l'utilisation de ce matériel même si nous étions, ou aurions dû être, au courant de la possibilité des dommages.

Certains liens de cette trousse font référence à des sites web ou articles qui ne sont pas sous le contrôle de Cybereco. Cybereco n'est pas responsable du contenu de ces sites web, ni des informations, logiciels, produits et services disponibles sur ou par l'intermédiaire de ces sites. Les liens sélectionnés sont uniquement destinés à fournir un complément d'information. Cybereco n'assume aucune obligation ou responsabilité de quelque nature que ce soit à cet égard.

Cette exonération de responsabilité vaut pour Cybereco et chacun des membres Cybereco ainsi qu'à notre personnel, nos consultants et à leur personnel et leurs consultants respectifs.