MEMO

L'HAMEÇONNAGE

1/4

Quésako ?

L'hameçonnage est une technique frauduleuse par laquelle un escroc veut vous faire croire qu'il est une personne ou une institution que vous connaissez et en qui vous avez confiance — banque, administration, contact personnel… — afin de vous soutirer des renseignements privés ou professionnels.

Son but ?

- Récupérer des informations personnelles comme vos identifiants, mots de passe, numéros de carte de crédit
- Accéder à des données sensibles au sein de la Ville
- Obtenir un transfert d'argent

Comment ?

En vous téléphonant, ou en vous envoyant un e-mail ou un message contenant :

- Une pièce jointe infectée qui installe un virus sur votre appareil
- Un lien qui redirige vers un site malicieux
- Un faux système de paiement

MEMO

L'HAMEÇONNAGE

2/4

Démasquez un e-mail de phishing

Soyez vigilant. Certains éléments doivent vous alerter :

- Il n'y a aucune raison que vous receviez ce message
- L'objet de l'e-mail est vague, vous n'identifiez pas le contexte
- Il est arrivé dans vos spams
- Il est question d'une récompense ou d'une sanction potentielle
- Le ton est alarmiste ou intriguant et joue sur le besoin d'une réponse urgente

MEMO

L'HAMEÇONNAGE

3/4

Adoptez les bons réflexes contre le phishing

- Ne répondez pas à l'e-mail
- Vérifiez la conformité de l'adresse expéditeur en positionnant le curseur de votre souris dessus, sans cliquer.
- Ne cliquez pas sur les liens. Positionnez le curseur de votre souris dessus, sans cliquer, pour vous assurer qu'il s'agit de l'adresse du site officiel de l'organisation
- N'ouvrez pas les pièces jointes, fichiers ou images
- N'effectuez aucune transaction via un système inconnu
- Mettez vos données à l'abri et faites des sauvegardes régulièrement
- Discutez-en avec vos collègues
- Transférez l'e-mail à **irisline@cirb.brussels**

MEMO

L'HAMEÇONNAGE

4/4

Réagissez si vous pensez être victime d'une attaque par phishing

Dans le cadre professionnel,

- Envoyez immédiatement un e-mail à **irisline@cirb.brussels**
- Prévenez votre chef et vos collègues

Dans le cadre privé,

- Contactez la personne ou l'organisation usurpée via un autre canal
- Changez vos mots de passe
- Si vous avez communiqué des données sur vos moyens de paiement, faites opposition auprès de votre organisme bancaire
- Faites un check anti-virus sur votre ordinateur
- Contactez le Centre pour la Cybersécurité Belgique (CCB) **https://www.safeonweb.be**