Phishing : Présentation du processus

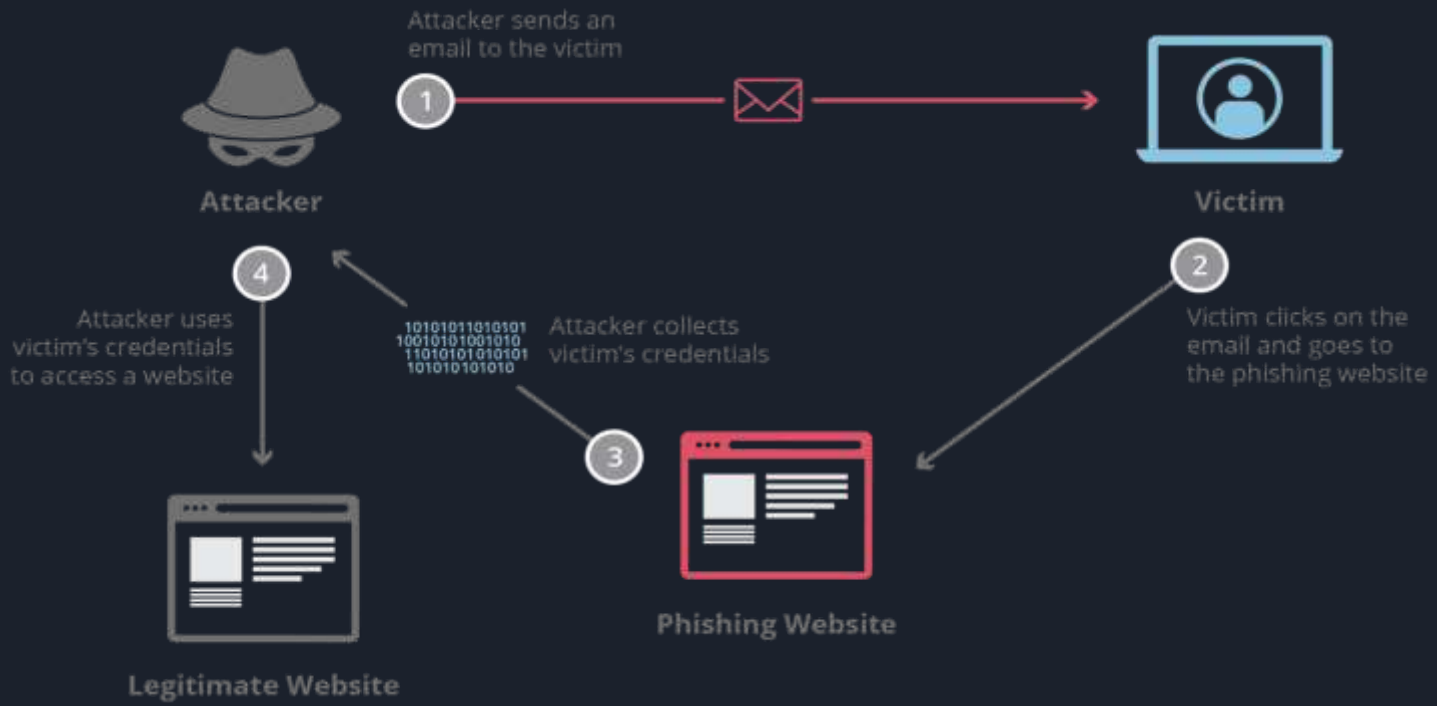
Participant :

- Hakan Aysan

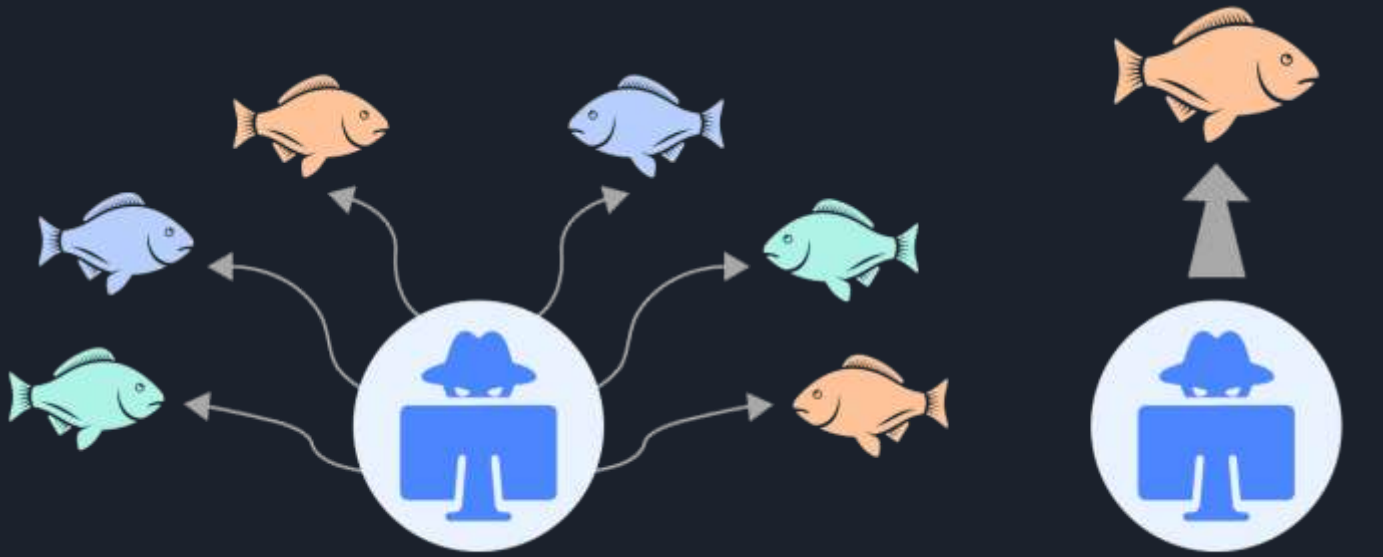
Supervisé par :

- M. Benoît Parthoens
- Mme. Julie Van de Wijngaert

Qu’est ce que le Phishing ?



Qu’est ce que le Spear Phishing ?



Phishing

Spear Phishing

Comment identifier un mail de phishing ?

Noms de domaine

- https://www.ing.be
- http://https.www.argenta.be.madlart.com/nl/aanvraag

Caractéristiques des messages de phishing :

- Côté inattendu
- Caractère urgent
- Attise la curiosité
- En-tête impersonnel
- Demande de cliquer sur un lien ou d'ouvrir une pièce jointe
- Demande de fournir des données personnelles

Exemple de mail de phishing

De : Belfius Banque [mailto:belfiusbanque@intl.be]
Envoyé le : lundi 7 janvier 2013 13:03 1
A : Xxxxxxx
Objet : Votre Online Banking est temporairement bloqué

Brussels,07 januari, 2013

Votre Online Banking est temporairement bloqué

Cher client

Votre banque en ligne est temporairement bloqué Nous avons récemment votre compte, et pensons que votre Belfius Banque account serait approché par un tier non autorisé. La sécurité de votre compte est notre principale préoccupation. Par conséquent, à titre préventif, nous avons temporairement un accès limité au fonctions sensibles du compte. Pour rétablir l'accès à votre compte, nous avons besoin de vous pour confirmer votre identité. Pour ce faire nous avons besoin de vous pour suivre le lien ci-dessous et confirmer vos informations : authentifier en cliquant sur le lien suivant.

https://www.belfius.be/info/NL/KlantWorden/index.aspx

Nous vous remercions de votre patience pendant que nous travaillons ensemble pour protéger votre compte. Après avoir rempli les informations requises, votre banque en ligne est mis à jour automatiquement avec le nouveau logiciel. Une fois que vous avez fait cela, vous êtes contacté par téléphone par l'un des employés du département internet banking, pour installer le logiciel. Rappelez-vous, Belfius Banque s'est engagée à votre sécurité et protection. 2

merci pour votre temps et coopération,

3

Cordialement,
2011 BELFIUS Conditions légales et informations 4

Pourquoi cet e-mail est-il un faux ?

1. L'adresse e-mail de l'expéditeur, à savoir « ...@intl.be », n'est pas une adresse e-mail de Belfius. Il peut également s'agir d'une adresse e-mail inconnue de Belfius (exemple : .info@belfius.be)
2. Le lien présent dans l'e-mail (https://www.belfius.be/...) semble correct par son contenu, mais lorsque vous vous positionnez dessus (sans cliquer) au moyen de la souris, une tout autre adresse apparaît (http://pmausa.com/... dans le présent exemple, mais il peut s'agir d'une autre adresse « non-Belfius »).
3. De manière générale, le texte de l'e-mail n'est pas toujours rédigé dans un langage correct.
4. La signature de l'e-mail contient des données erronées concernant un service ou une personne de contact.

En pratique, nous constatons que l'élément 2 et un des autres éléments ne sont pas corrects.

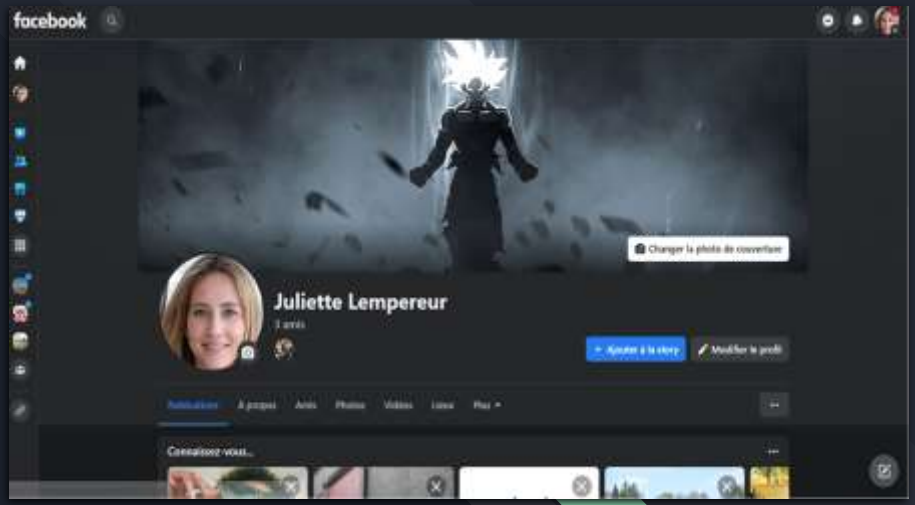
Objectifs et porté de la campagne de phishing

- Sensibiliser
- Former
- Évaluer

Mode opératoire

Tentative n°1

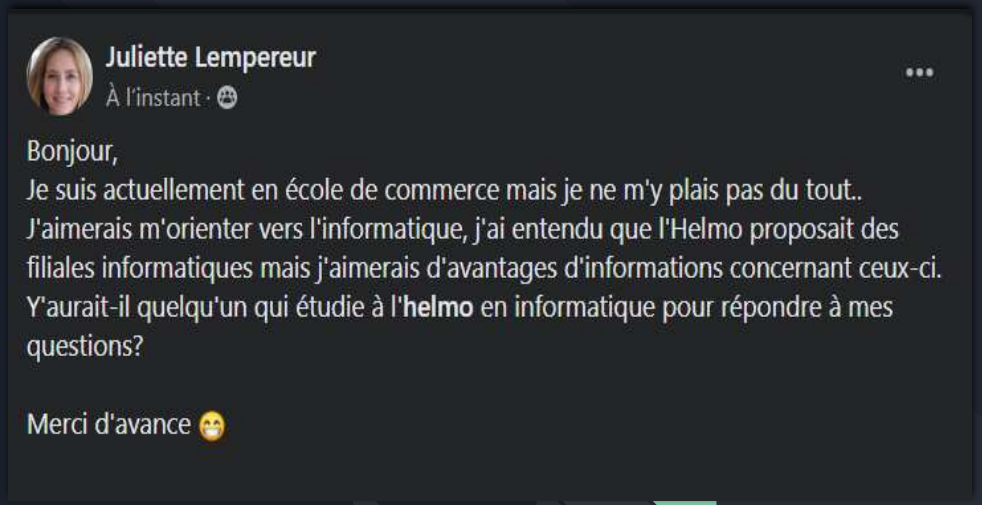
- Cible : Tout étudiant d'informatique à l'Helmo
- Objectif : Récupérer un horaire de B1
- Informations nécessaire à cette tentative :
    * Création d'un faux compte Facebook
    * Inscription au groupe "Etudiants de Liège"



Tentative n°1

Scénario :

* Publier sur le groupe “Etudiants de Liège “
* Se faire passer pour une élève de marketing
* Attirer un étudiant

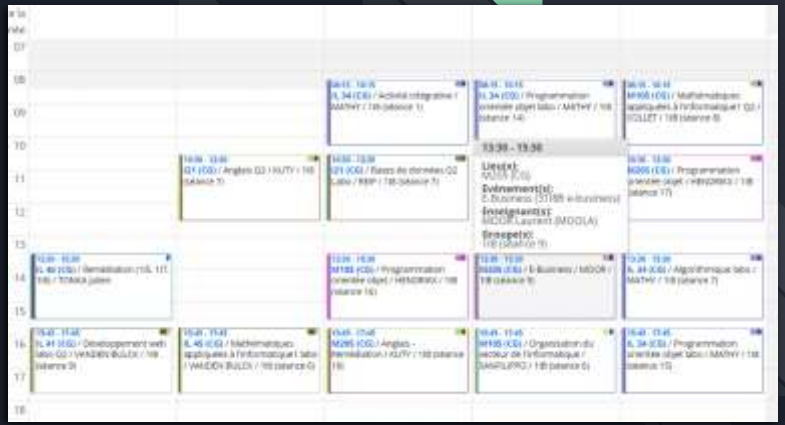


Résultats ?

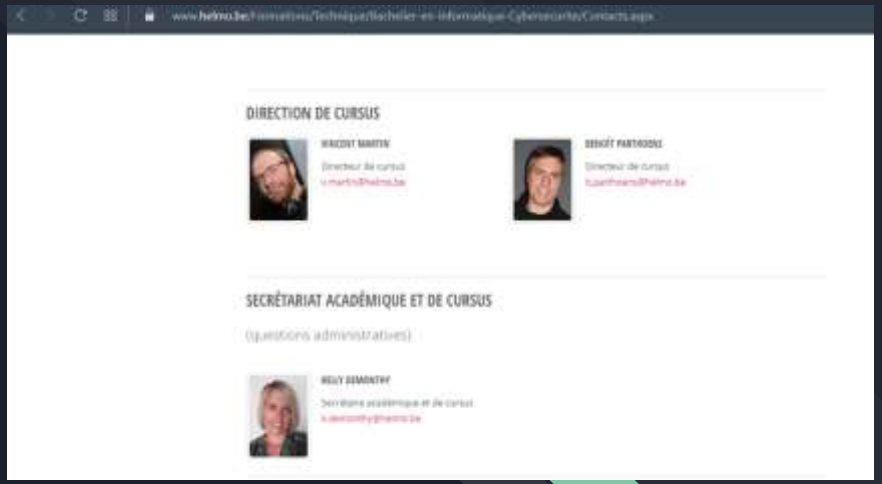
Résultats: Tentative n°1

- 4 réponses sous la publication
- 1 seul étudiant de HELMO en informatique de Gestion

➔ Obtention de l'horaire du groupe 8



Tentative n°2



- Cible : Secrétaire d'HELMO
- Objectif : Récupérer la liste des étudiants de B1 Info & Sécu
- Informations nécessaires à cette tentative :
    * Adresse mail de la secrétaire
    * Création d'une fausse adresse mail

Tentative n°2

- Événement Cybersécurité à Bruxelles le 19/20 avril.

Scénario :

* Envoyer un mail à la secrétaire
* Se faire passer pour un organisateur de l’évènement
* Inviter les étudiants de B1 du cursus informatique

Résultats ?

Résultats: Tentative n°2

- Aucune réponse de la secrétaire

Aucune liste d’étudiants

Tentative n°3

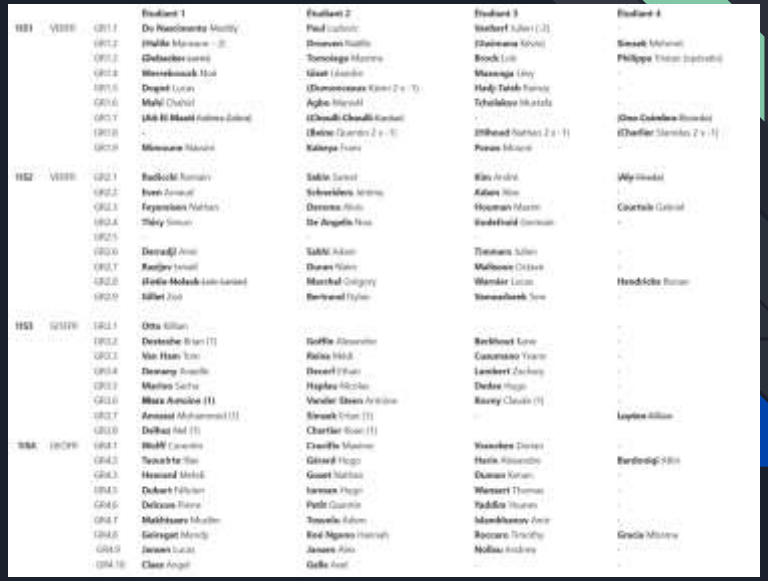
- Cible : Étudiant de B1 Sécu
- Objectif : Récupérer la liste des étudiants de B1 Sécu
- Information nécessaire à cette tentative :

- Complice proche d’un étudiant

Résultats ?

Résultats: Tentative n°3

- Récupération de la liste par le complice



Tentative n°4

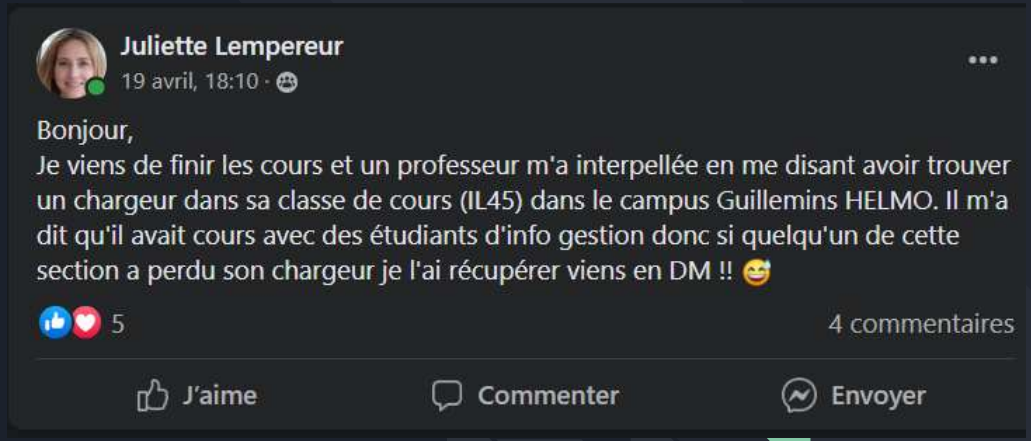
- Cible : Étudiant de B1 Info
- Objectif : Récupérer la liste des étudiants de B1 Info
- Information nécessaire à cette tentative :

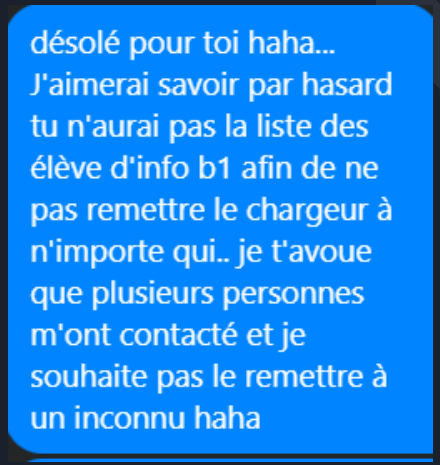
- Faux compte Facebook créer plus tôt
- Groupe Facebook “Etudiants de Liège”
- Horaire B1 Info

Tentative n°4

Scénario :

- Se rendre à un cours de B1 Info
- Oublier son chargeur
- Poster que nous détenons son chargeur.



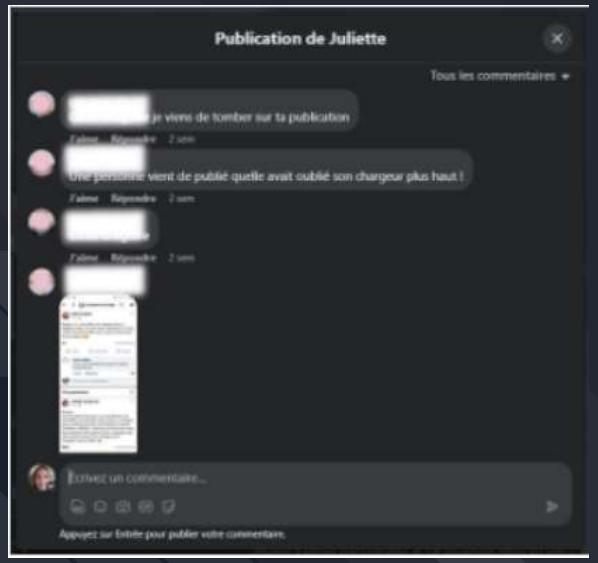


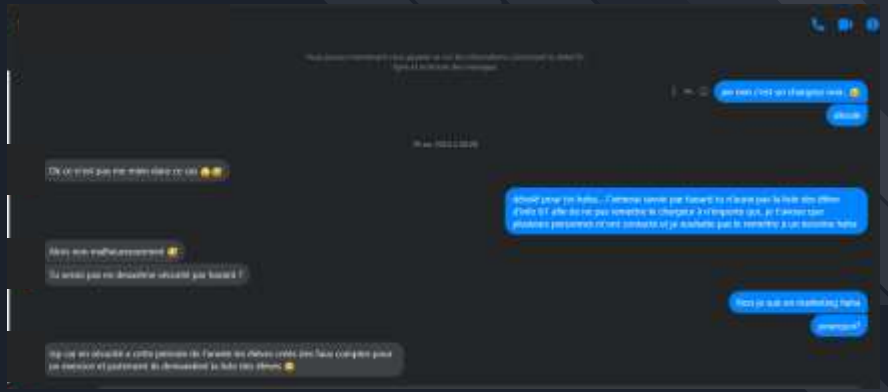
Selon vous, la tentative n°4 va-t-elle se conclure par un échec ou une réussite ?

Résultats: Tentative n°4

- Plusieurs réponses sous le tweet ciblant un étudiant
- Aucun résultat obtenu

=> au courant de la campagne





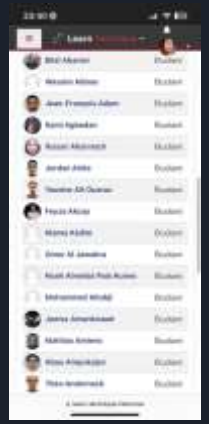
Tentative n°4 (Bis)

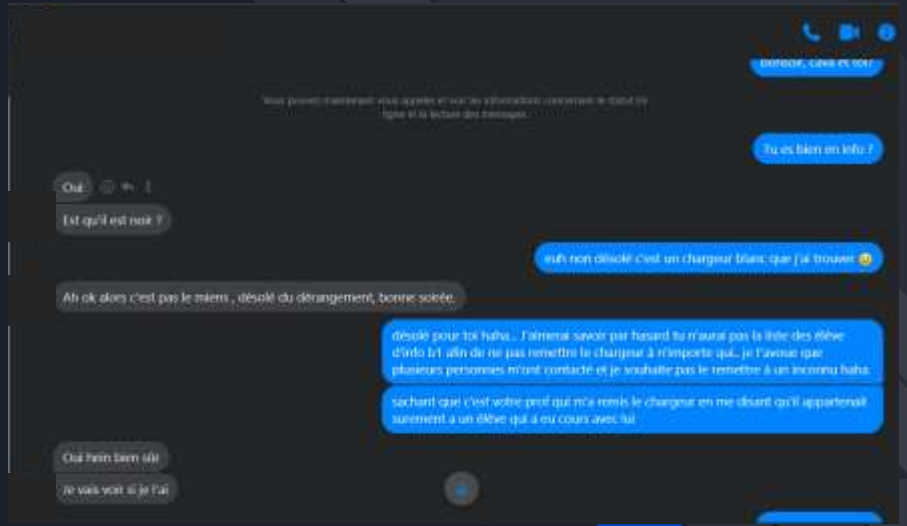
Même scénario que la tentative précédente

Message reçu de la part d’un B1 Info disant avoir perdu son chargeur

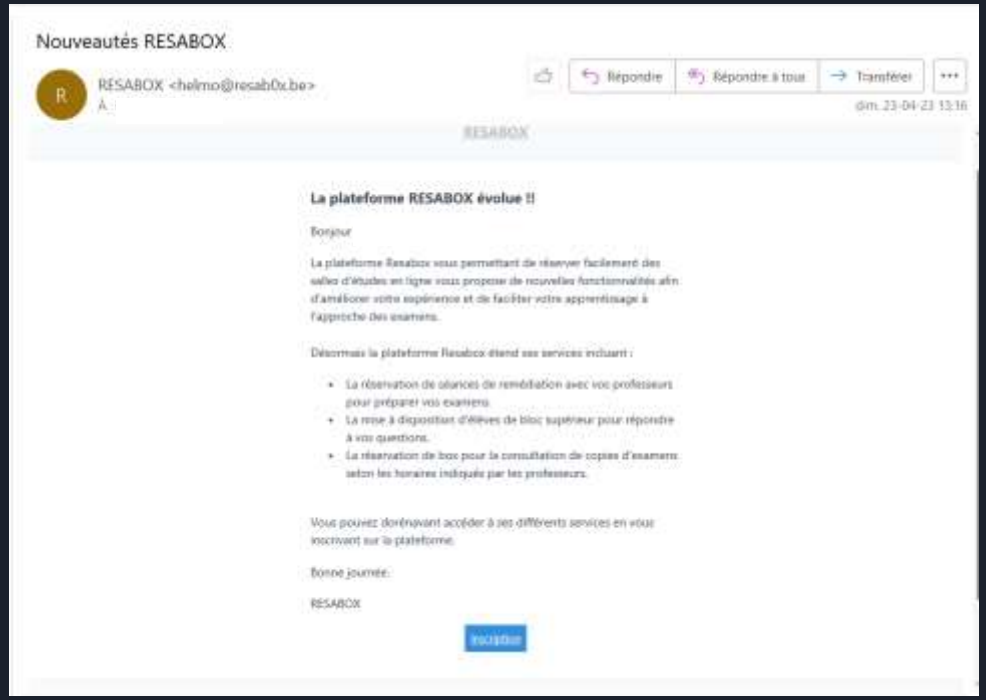
Résultats: Tentative n°4(bis)

- Étudiant coopératif face au scénario
- Liste obtenue





Mails envoyés aux étudiants



Nouveautés RESABOX

R RESABOX <helmo@resab0x.be>
À

Répondre | Répondre à tous | Transférer | ...

dim. 23-04-23 13:16

RESABOX

La plateforme RESABOX évolue !!

Bonjour

La plateforme Resabox vous permettant de réserver facilement des salles d'études en ligne vous propose de nouvelles fonctionnalités afin d'améliorer votre expérience et de faciliter votre apprentissage à l'approche des examens.

Désormais la plateforme Resabox étend ses services incluant :

- La réservation de séances de remédiation avec vos professeurs pour préparer vos examens.
- La mise à disposition d'élèves de bloc supérieur pour répondre à vos questions.
- La réservation de box pour la consultation de copies d'examens selon les horaires indiqués par les professeurs.

Vous pouvez dorénavant accéder à ces différents services en vous inscrivant sur la plateforme.

Bonne journée.

RESABOX

Inscription

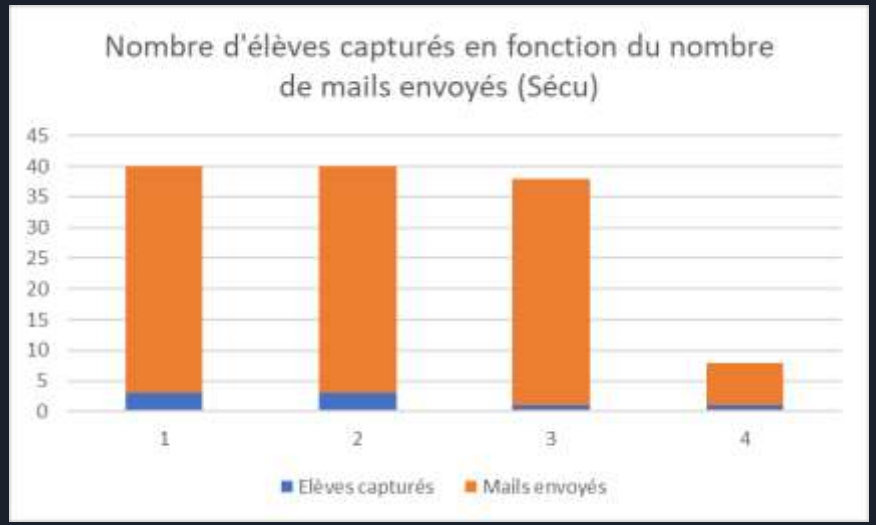
Résultats personnels

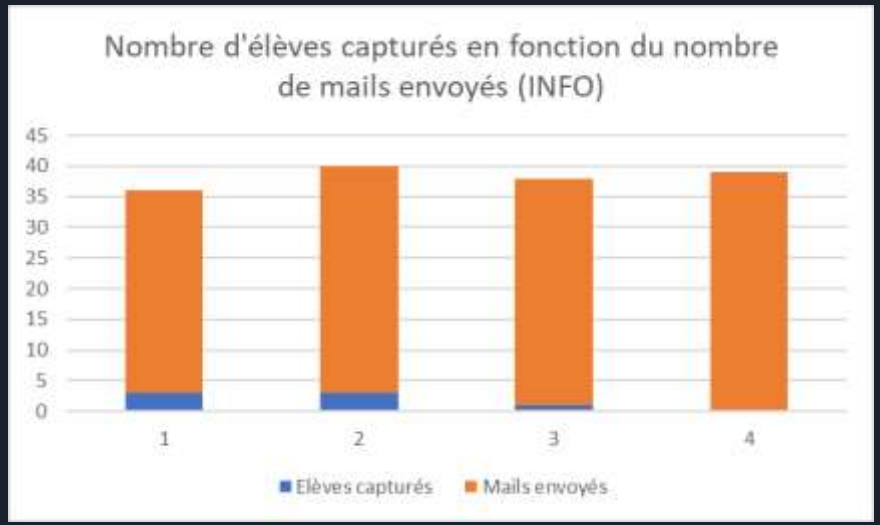
Mails envoyés: 37 mails

Etudiants capturés: 3 étudiants

Réussite: 8,1%

Résultats généraux





Total : 9/118 ⇨ 7,6 %

Total: 8/189 ⇨ 4,2 %

Quels seraient, selon vous, les bons réflexes à adopter pour se prémunir contre une attaque de phishing ?

Réflexes et recommandations

- Être vigilant face aux e-mails inattendus
- Vérifier les URL avant de cliquer
- Vérifier l’adresse mail d’envoi
- Utilisez l'authentification à deux facteurs
- Mettez à jour régulièrement les logiciels de sécurité
- Ne pas ouvrir de pièce jointe dans un mail “douteux”

Avez-vous déjà été victime de Phishing (hors-cours) ?

Comment avez-vous réagi face au mail de phishing reçu ?

Merci pour votre attention !