

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?



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 A :Xxxxxxxxx

Objet: Votre Online Banking est temporairement bloqué

Brussels.07 januari, 2013

Votre Online Banking est temporairement bloqué.

Cher plent

Votre banque en ligne est temporarement bloqué Nous avons récemment votre compte, et pensons que votre Betflus. 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.beffius.be/info/NL/KlantWorden/index.aspx

Nous vous remercions de votre patience pendant que nous tra par ensemble pour protéger votre compte. Après avoir rempli les informations requises, votre banque en ligne est mis par la utomatiquement 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. Belflus Sangue s'est engagée à votre sécurité et protection.

merci pour votre temps et coopération,





Pourquoi cet e-mail est-il un faux 7

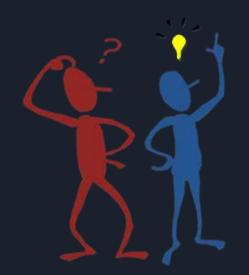
- 13 Cadreuse e-mail de l'expéditeur, à savoir « . Eliret be », riest pus une adreuse e-mail de fielfusi. Il peut équiement s'ager d'une adresse e-mail inconnue de Belfius lexemple: info@belfius bel-
- Le lien présent dans l'e-mail (https://www.belfus.be/...) semble correct par son conceru, mars lorsque vous vous positionnes. dessus (lians sliguer) as moven de la souris, une tout autre adresse apparait (http://b/mausa.com/, dans le présent exemple, mais if peut s'agr d'une autre adresse « non-Belfius »)
- De manière générale, le texte de l'e-mai réest pas toussurs rédigé dans un language correct.
- La signature de l'e-mail consient des données erronées concernant un service ou une personne de contact.

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

Objectifs et porté de la campagne de phishing

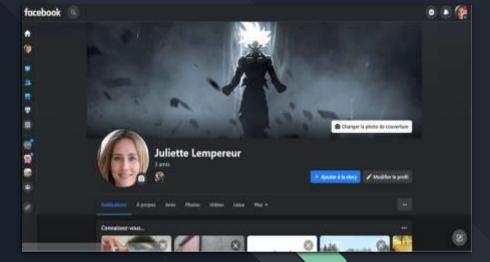
- Sensibiliser
- Former
- Évaluer

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"





Scénario:

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



Juliette Lempereur

Bonjour,

Je suis actuellement en école de commerce mais je ne m'y plais pas du tout. J'aimerais m'orienter vers l'informatique, j'ai entendu que l'Helmo proposait des filiales informatiques mais j'aimerais d'avantages d'informations concernant ceux-ci. Y'aurait-il quelqu'un qui étudie à l'helmo en informatique pour répondre à mes questions?

Merci d'avance 😁

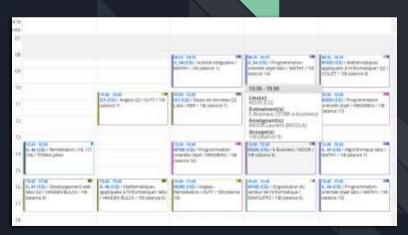
Résultats?





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

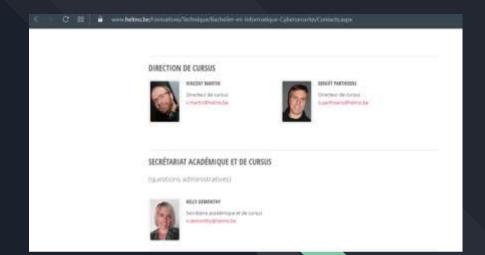
• Cible : Secrétaire d'HELMO

• 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

			Biodiest 1	Enallant 2	Studieré 3	Electrical d
1101	YES	1.1/00	Do Nacobeanty Mustry	Ped cubot:	Westwerf Julier (12)	
		1,000	projekt blancom - 21	Deserved Suprise	(Challenging School)	Simont Mahamat
		0013	Chilarkor (1970)	Tomolege Murris	Brook Lills	Philippe Vision Instrums
		08th	Westermark No.	Wast Learning	Manufage (1907)	
		187.5	Degree Corps	(Dismonorana Cont. 7 to 17)	Hardy Takels Number	
		6606	Mark Charlet	Aghe-Hirotti	Tehnilalogo litt. a tala	
		080.7	Mile Hil Mantel Follows Collect	(Chroult Chroal) Karteri		(One Colvelar Street)
		1903	42.00	Obeing Guerrin 2 y - 10	Ettibood Sunney 2 s - 11	(Charlier Stember 2 v -1)
		Met.s	Minesane Nation	Kallerga Franci	Person Inforces	
1107	VIII	190.1	Budlock Names	Sable Same	Wiley Archite.	Welledge
		signt.t.	Part Assessed	Schoolders terring	Alders Nov.	117
		ORLE	Ferencision Numbers	Deroma Mido	Houman Marri	Coortale Ground
		180.6	Thirty Some	the dangelin Nova	Reside Could Communicate	F-1
		1852.5				
		1800	Derradi /mm	TARK NAME	Timerana fullers	
		OFULT	Region to half	Dunary States	Wellsowe Cittles	
		480.0	(Feth Holish in brind	Manthal Collegory	Warnier Louise	Hendricke house
		992.9	Siller 200	Betweel N/m	Monascheek Sco	
1153	121176	184.1	Otto Gillan			
		DESCRIPTION	Destender Braziliti	Boffle Country	Barkhood Love	
		OFO.5	Non-Ham-Total	Ratina Middl	Cusumano Yvaro	
		080.4	Demany Louds	Depart Char	Landbert Assistant	
		GR(1)	Warten Softer	Hapley (School	Dedes these	
		GRILLI	Marx Amoire (1)	Vander Steen Antonio	Binarry Chronin (9)	
		oto.r	American Multiprocessor (11)	Street Stor (1)		Lauries dillion
		GP(1)0	Delhas hid (1)	Chartier (con (1)		
164	reces	1911	Block Concerns	Deritte Maximum	Wanning Done	
		0843	Tenah te Soi	Gitaril Hogo	Harin, Filtramotor	Berdonigi S Rivi
		GRO.	Hemised Motoli	Good Nathan	Ocean Kerters	
		DRACE	Diction to February	former Pego	Westerl Thomas	
		GRAD	Delouse France	Pyele Guerrin	Yaddin Human	
		ONAT	Mathematical Continues of the Control of the Contro	Topovelo falore	Informition and Print	
		1204.8	Selreget Monto	Red Nigero Herryly	Recome Timothy	Grade Mistery
		684.9	Services busins	Janess Pinn	Modina Archive	

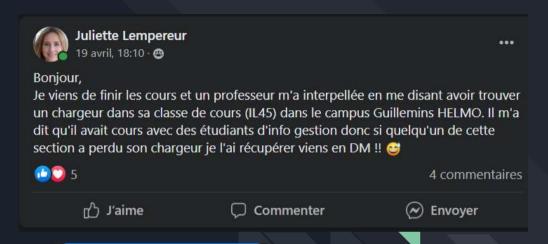
Tentative n°4

- 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.



désolé pour toi haha...
J'aimerai savoir par hasard
tu n'aurai pas la liste des
élève d'info b1 afin de ne
pas remettre le chargeur à
n'importe qui... je t'avoue
que plusieurs personnes
m'ont contacté et je
souhaite pas le remettre à
un inconnu haha

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



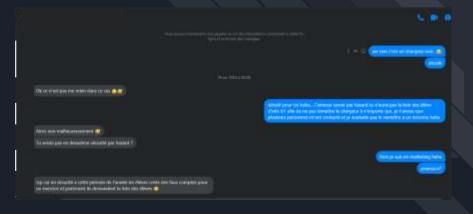


Résultats: Tentative n°4

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

=> au courant de la campagne

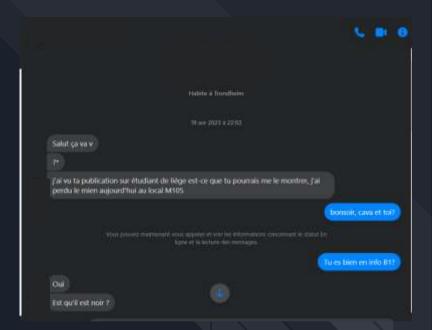




Tentative n°4 (Bis)

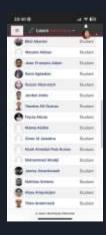
Même scénario que la tentative précédente

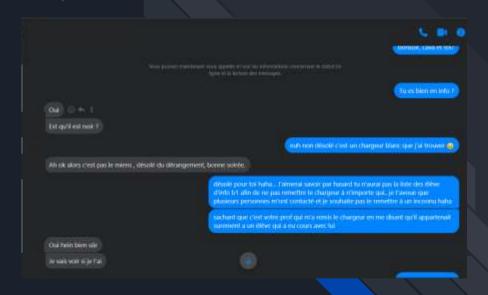
Message reçu de la part d'un B1 Info disant avoir perdu son chargeur



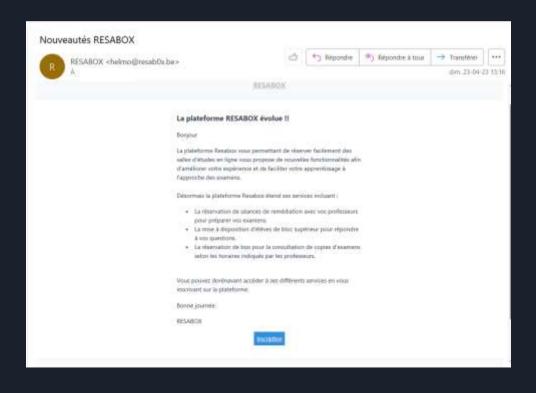
Résultats: Tentative n°4(bis)

- Étudiant coopératif face au scénario
- Liste obtenue





Mails envoyés aux étudiants



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!

