UQAC
Université du Québec
à Chicoutimi

DÉVELOPPEMENT ET ÉVALUATION D'UN JEU SÉRIEUX POUR LA SENSIBILISATION À L'HAMEÇONNAGE MOBILE

PAR ELVIS NOEL IRAMBONA

MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À CHICOUTIMI EN VUE DE L'OBTENTION DU GRADE DE MAÎTRISE ÈS SCIENCES (M. Sc.) EN INFORMATIQUE

QUÉBEC, CANADA

RESUME

Ce travail de recherche porte sur le développement et l'évaluation d'un jeu sérieux visant à sensibiliser les utilisateurs à l'hameçonnage mobile, une menace croissante dans le domaine de la cybersécurité. Avec la prolifération des smartphones et l'augmentation des attaques de type smishing (hameçonnage par SMS), il devient impératif de mettre en place des outils pédagogiques efficaces pour éduquer les utilisateurs aux bonnes pratiques de cybersécurité.

L'objectif principal de ce mémoire est de concevoir, développer et évaluer un jeu sérieux interactif permettant aux utilisateurs d'identifier et de réagir face à des tentatives d'hameçonnage mobile. Le projet repose sur une approche de conception centrée sur l'utilisateur, combinant des principes de gamification et des méthodes pédagogiques adaptées pour renforcer l'apprentissage.

La méthodologie adoptée s'appuie sur le modèle du Design Thinking et les méthodes agiles pour assurer une conception itérative du jeu. Le développement du prototype a été réalisé avec le moteur de jeu Construct 3, facilitant la création d'une expérience immersive et accessible sur plateformes mobiles. L'évaluation du jeu a été menée à travers des tests finaux impliquant 20 participants et une analyse des résultats issus de questionnaires préliminaires et post-intervention.

Les résultats obtenus ont montré une amélioration significative des capacités des utilisateurs à identifier des tentatives d'hameçonnage mobile après avoir joué au jeu. Ce mémoire met en évidence le potentiel des jeux sérieux comme outils de sensibilisation à la cybersécurité et ouvre la voie à de futures recherches sur l'amélioration et l'extension de ce type de solutions éducatives.

ABSTRACT

This research focuses on the development and evaluation of a serious game aimed at raising user awareness of mobile phishing, a growing threat in the field of cybersecurity. With the proliferation of smartphones and the rise of smishing attacks (SMS phishing), it has become crucial to implement effective educational tools to teach users good cybersecurity practices.

The main objective of this study is to design, develop, and evaluate an interactive serious game that enables users to identify and appropriately respond to mobile phishing attempts. The project is based on a user-centered design approach, combining gamification principles and adapted pedagogical methods, to strengthen learning outcomes.

The adopted methodology relies on the Design Thinking model and agile methods to ensure an iterative design process. The game prototype was developed using the Construct 3 game engine, facilitating the creation of an immersive and accessible experience on mobile platforms. The game's evaluation was conducted through final tests involving 20 participants, and an analysis of the results obtained from preliminary and post-intervention questionnaires.

The results showed a significant improvement in users' abilities to recognize mobile phishing attempts after playing the game. This thesis highlights the potential of serious games as effective tools for cybersecurity awareness and paves the way for future research on enhancing and expanding such educational solutions.

TABLE DES MATIERES

LISTE DES TABLEAUX

LISTE DES FIGURES

REMERCIEMENTS

En tout premier lieu, je tiens à exprimer ma profonde gratitude à Dieu, le Tout-Puissant, pour sa grâce et son soutien quotidien.

Je tiens également à remercier mon directeur de recherche, Monsieur Fehmi Jaafar, ainsi que mon co-directeur, Monsieur Bob-Antoine Jerry Ménélas, pour leur encadrement et leurs précieux conseils tout au long de cette recherche. Leur expertise et leur disponibilité ont été essentielles à l'aboutissement de ce travail.

À mes professeurs et à toute l'équipe administrative du département d'informatique et de mathématique de l'UQAC, mes sincères remerciements pour ce parcours de Maîtrise enrichissant. Votre dévouement a été essentiel à ma réussite.

Un immense merci à ma chère épouse et nos enfants, pour leur patience et leur compréhension tout au long de cette aventure académique.

Je souhaite aussi témoigner ma reconnaissance à mes amis, en particulier à Monsieur Christian Lamonde, pour leur bienveillance, leur aide et les discussions enrichissantes qui ont jalonné ce parcours.

Enfin, je remercie toutes les personnes ayant participé à l'évaluation de ce jeu sérieux, ainsi que ceux qui ont contribué, de près ou de loin, à la réalisation de cette recherche.

CHAPITRE I

INTRODUCTION

1.1 PROBLEMATIQUE

L'évolution rapide des technologies mobiles a considérablement amélioré nos vies quotidiennes, mais a également ouvert de nouvelles opportunités pour les cybercriminels. L'hameçonnage mobile (« mobile phishing », en anglais), une forme de fraude en ligne, représente une menace croissante, exploitant la vulnérabilité ou l'inattention des utilisateurs sur leurs appareils portables (Goel & Jain, 2018). Selon le rapport de Verizon (2023), 74 % des violations de données impliquent l'élément humain. Face à cette menace, il est impératif de développer des stratégies innovantes pour sensibiliser et protéger les individus contre les attaques d'hameçonnage mobile.

L'ampleur de l'hameçonnage mobile se reflète dans le nombre croissant d'incidents signalés (Centre de la sécurité des télécommunications, 2021) et la diversification des techniques utilisées par les cybercriminels (Trudel et al., 2007 ; Schafer, 2018). Les dispositifs mobiles, tels les téléphones intelligents (« smartphones », en anglais) et les tablettes, sont devenus des cibles privilégiées en raison de leur omniprésence et de la quantité considérable d'informations personnelles qu'ils stockent (Goel & Jain, 2018). En effet, la plupart de personnes ont désormais tendance à utiliser les appareils mobiles pour des activités qui autrefois étaient effectuées sur ordinateurs (Verkijika, 2019). Par conséquent, la nécessité d'éduquer les utilisateurs sur les risques spécifiques de l'hameçonnage mobile et de promouvoir des comportements sécurisés est plus nécessaire que jamais (Centre de la sécurité des télécommunications, 2020; Goel & Jain, 2018; Schafer, 2018; Trudel et al., 2007; Verkijika, 2019).

La problématique centrale de ce mémoire réside dans la recherche de moyens efficaces pour sensibiliser les utilisateurs aux menaces d'hameçonnage mobile et encourager des pratiques de sécurité adéquates. Comment concevoir un outil pédagogique qui puisse à la fois captiver l'attention des utilisateurs et leur fournir des connaissances pratiques pour détecter et éviter les

attaques d'hameçonnage sur leurs appareils mobiles ? Comment mesurer l'impact réel d'un tel outil sur l'acquisition de compétences en matière de sécurité et sur le comportement des utilisateurs dans un contexte réel ?

Les jeux sérieux émergent comme des instruments prometteurs dans le domaine de la sensibilisation à la sécurité en ligne (Onashoga et al., 2019). Cependant, il reste une lacune significative dans la littérature et la recherche empirique quant à la conception, le développement et l'évaluation de jeux sérieux pour lutter spécifiquement contre l'hameçonnage mobile. Ce mémoire s'engage à combler cette lacune en explorant de manière approfondie la potentialité des jeux sérieux en tant qu'outil éducatif pour la prévention de l'hameçonnage mobile. En outre, cette recherche s'interrogera sur la manière dont les caractéristiques ludiques des jeux sérieux peuvent influencer positivement l'efficacité pédagogique.

Ce mémoire s'inscrit dans une démarche multidisciplinaire, combinant les domaines de la cybersécurité, de la psychologie de l'apprentissage, et du design de jeux, pour élaborer des solutions innovantes qui répondent de manière adaptative et engageante aux défis posés par l'hameçonnage mobile. En confrontant ces aspects, cette recherche aspire à contribuer significativement à l'enrichissement des connaissances dans le domaine de la sensibilisation à la sécurité en ligne, avec des implications concrètes pour la protection des utilisateurs face aux menaces croissantes de cette forme d’attaque.

1.2 OBJECTIFS DE RECHERCHE

1.2.1 OBJECTIF PRINCIPAL

Le travail de recherche proposé a pour but de concevoir, développer et évaluer *SafeMobile Adventure*, un jeu sérieux pour la sensibilisation et la prévention de l'hameçonnage mobile. Le jeu sérieux vise notamment à renforcer la compréhension des utilisateurs face aux risques de sécurité, et à promouvoir des comportements sécuritaires sur les appareils mobiles.

1.2.2 SOUS-OBJECTIFS

La mise en œuvre du jeu sérieux passera par la réalisation de certaines étapes :

- Effectuer une analyse approfondie des techniques d'hameçonnage mobile et des pratiques de sécurité en ligne pour alimenter le développement du jeu sérieux.
- Concevoir et développer un jeu sérieux interactif et engageant, intégrant des scénarios réalistes d'hameçonnage mobile tout en fournissant des conseils pratiques pour éviter ces situations.
- Évaluer l'efficacité du jeu sérieux en ce qui concerne l'acquisition de connaissances, la modification des comportements et l'amélioration de la perception de la sécurité en ligne chez les utilisateurs.
- Recueillir et analyser les retours des utilisateurs afin d'itérer et d'améliorer le jeu sérieux pour optimiser son impact éducatif et son accessibilité.
- Fournir des recommandations pour l'intégration et l'utilisation efficace du jeu sérieux comme outil de sensibilisation à la sécurité en ligne, en mettant en évidence ses bénéfices potentiels pour les utilisateurs et les professionnels de la cyber sécurité.

1.3 APPROCHE METHODOLOGIQUE

L'approche méthodologique de cette thèse adopte une démarche mixte, combinant des méthodes qualitatives et quantitatives pour examiner de manière approfondie l'efficacité d'un jeu sérieux dans la prévention de l'hameçonnage mobile.

La première étape implique une revue exhaustive de la littérature pour établir une base solide. Celle-ci identifie les lacunes existantes et certaines pratiques dans les domaines de l'hameçonnage mobile, des jeux sérieux en éducation, et de la sécurité en ligne.

La méthodologie comprend ensuite une phase d'analyse des besoins, s'appuyant sur les avis des experts en cybersécurité et des concepteurs de jeux sérieux, afin de définir les exigences spécifiques pour la prévention de l'hameçonnage mobile. Cette étape alimente la conception du

prototype interactif du jeu sérieux, intégrant des mécanismes de jeu engageants et des scénarios réalistes d'hameçonnage mobile.

Le développement du prototype est suivi par des tests initiaux, impliquant un échantillon représentatif d'utilisateurs, pour évaluer l'expérience utilisateur et la jouabilité. Les retours des utilisateurs guident ensuite des itérations rapides pour améliorer le prototype. Une fois la version finale du jeu sérieux prête, une évaluation finale est menée, avec un échantillon plus large, pour évaluer de manière approfondie son efficacité en termes d'acquisition de connaissances et de modification des comportements.

L'analyse des résultats de l'évaluation, combinant des méthodes quantitatives et qualitatives, nourrira la rédaction du mémoire, présentant des conclusions sur l'efficacité du jeu sérieux, ses implications pratiques et des recommandations pour les futures recherches.

Cette approche méthodologique vise à contribuer de manière significative à la compréhension et à l'application des jeux sérieux dans le contexte spécifique de la sensibilisation et de la prévention de l'hameçonnage mobile.

1.4 ORGANISATION DU MEMOIRE

Ce mémoire est structuré en plusieurs chapitres qui suivent une progression logique du projet, de l'identification du problème jusqu'à l'évaluation de la solution développée. Le premier chapitre introduit le contexte général de l'hameçonnage mobile, présente la problématique, les objectifs de recherche ainsi que la méthodologie adoptée. Il se termine par la présente section qui décrit la structure globale du document.

Le second chapitre est consacré à la revue de la littérature. Il explore en profondeur les notions liées à l'hameçonnage mobile, les initiatives existantes en matière de sensibilisation, ainsi que les fondements théoriques des jeux sérieux.

Le troisième chapitre expose l'analyse des besoins pédagogiques et techniques, ainsi que les éléments de conception du jeu. Il présente les choix de design, les types de scénarios d'hameçonnage intégrés et les mécanismes d'apprentissage envisagés.

Le quatrième chapitre décrit le développement du prototype du jeu. Il détaille les technologies et outils utilisés, les fonctionnalités essentielles, l'interface utilisateur, ainsi que le calendrier de développement.

Le cinquième chapitre présente les tests finaux et l'évaluation de l'efficacité du jeu. Il décrit la méthodologie d'évaluation, les instruments utilisés, les données recueillies auprès des participants et l'analyse des résultats obtenus. Ce chapitre discute également des résultats à la lumière des objectifs initiaux, et met en évidence les points forts du jeu ainsi que les pistes d'amélioration.

Le sixième chapitre, enfin, conclut le mémoire en relatant les grandes lignes de ce projet, et en proposant des perspectives pour des travaux futurs dans le domaine de la sensibilisation à l'hameçonnage mobile par le jeu sérieux.

CHAPITRE II

REVUE DE LA LITTERATURE

Ce chapitre propose une analyse approfondie des concepts clés qui forment le cadre théorique de cette recherche sur le développement et l'évaluation d'un jeu sérieux pour la sensibilisation à l'hameçonnage mobile. La revue de la littérature est structurée autour de trois axes principaux : l'hameçonnage mobile, les jeux sérieux et les travaux similaires.

2.1 HAMEÇONNAGE MOBILE

2.1.1 INTRODUCTION

L'hameçonnage mobile, une menace de plus en plus sophistiquée dans le paysage cybernétique contemporain (Canada, 2021; Trudel et al., 2007), constitue une forme spécifique d'attaque visant les utilisateurs d'appareils mobiles tels que les smartphones et les tablettes. Le Centre Canadien pour la cybersécurité (2022) décrit ce phénomène comme une pratique malveillante qui repose sur la tromperie des utilisateurs, en les incitant à divulguer des informations sensibles telles que les identifiants de connexion, les données bancaires ou les informations personnelles, en leur faisant croire qu'ils interagissent avec une entité légitime. Cette même organisation rapporte que les techniques d'hameçonnage mobile exploitent souvent des canaux de communication courants, tels que les messages textes, les courriels, les applications mobiles ou les réseaux sociaux, pour atteindre les utilisateurs (Centre Canadien pour la cybersécurité, 2022). En effet, les cybercriminels mettent en place des scénarios trompeurs, créant des répliques fidèles de sites web ou d'applications mobiles (Goel & Jain, 2018; Microsoft, 2024). Ces imitations peuvent être extrêmement convaincantes, induisant les utilisateurs en erreur et les incitant à agir de manière non sécuritaire.

Selon le Centre antifraude du Canada (2024) et OneSpan (2024), les messages d'hameçonnage mobile peuvent prendre diverses formes, notamment des notifications d'alerte

urgente, des offres séduisantes, ou des demandes d'authentification apparemment légitimes. L'objectif ultime des fraudeurs est de manipuler les utilisateurs pour qu'ils révèlent des informations confidentielles (Anna, 2022; Microsoft, 2024). Cet avis est partagé avec André (2023) qui précise que ces informations peuvent ensuite être exploitées à des fins frauduleuses, telles que le vol d'identité, le piratage de comptes bancaires, ou encore le détournement de fonds.

Pour Goel & Jain (2018), l'évolution rapide des technologies mobiles a ouvert de nouvelles opportunités pour les cybercriminels. Ils exploitent les faiblesses de sécurité des dispositifs mobiles qui sont devenus des compagnons omniprésents dans la vie quotidienne (Goel & Jain, 2018; Jain et al., 2022; Shahriar et al., 2015). De ce fait, l'usage intensif de certaines applications mobiles, la consultation des courriels et la réalisation de transactions financières via ces dispositifs en font des cibles attractives pour les attaquants.

Les techniques d'hameçonnage mobile évoluent constamment pour s'adapter aux tendances technologiques (Trudel et al., 2007). Dans leur article, (Goel & Jain, 2018) déplorent que des attaques utilisant des techniques d'hameçonnage via des applications mobiles frauduleuses sont de plus en plus fréquentes. Les utilisateurs peuvent être incités à télécharger des applications ou visiter des sites Web contrefaits, qui imitent souvent des services légitimes, mais qui sont conçues pour voler des informations sensibles une fois déployées sur leur dispositif mobile.

2.1.2 ORIGINES DE L'HAMEÇONNAGE MOBILE

D'après Purkait (2012), le terme « phishing » (« hameçonnage », en français) trouve ses racines dans le monde de la pêche, mais pas dans le contexte traditionnel de la capture de poissons. Celui-ci est en réalité une déformation du mot « fishing » (« pêche », en français) et a été utilisé pour décrire une méthode d'attaque informatique basée sur la tromperie et la ruse (Purkait, 2012).

Pour le Centre de la sécurité des télécommunications du Canada (2021), l'origine de l'hameçonnage est souvent associée à une attaque emblématique contre America Online (AOL) dans les années 1990, qui a marqué les premiers jours de cette technique d'escroquerie en ligne.

Goel & Jain (2018) appuie cette théorie et rapporte qu'en 1996, des cybercriminels ont lancé une attaque sophistiquée contre les utilisateurs d'AOL, l'un des fournisseurs de services Internet les plus populaires à l'époque. Cette attaque pionnière a été réalisée en créant de faux messages, semblables aux messages officiels d'AOL, incitant les utilisateurs à divulguer leurs informations de compte (Goel & Jain, 2018; Purkait, 2012).

A la suite à cet incident, le terme « phishing » a été forgé pour décrire cette forme spécifique d'attaque en ligne basée sur la tromperie (Goel & Jain, 2018). Purkait (2012) explique que la métaphore avec la pêche reflétait la manière dont les attaquants lancent des "hameçons" virtuels pour attraper des victimes potentielles. Cette attaque contre AOL a marqué le début d'une nouvelle ère, où les attaquants exploitent la confiance des utilisateurs en se faisant passer pour des entités légitimes (Centre de la sécurité des télécommunications, 2021). Depuis cette attaque, le phishing a évolué pour devenir une menace complexe et omniprésente dans le paysage de la cybersécurité, constate Ivanov et al. (2021).

Selon Shahriar et al. (2015), l'émergence de l'hameçonnage mobile est intimement liée à l'expansion des smartphones et des tablettes. En effet, les statistiques montrent qu'au courant des années 2000, l'utilisation des téléphones mobiles a connu une croissance exponentielle, accompagnée de l'accès à Internet via des réseaux mobiles (Laricchia, 2024). Le diagramme suivant donne un aperçu sur l'évolution annuelle du marché des smartphones depuis 2007 :

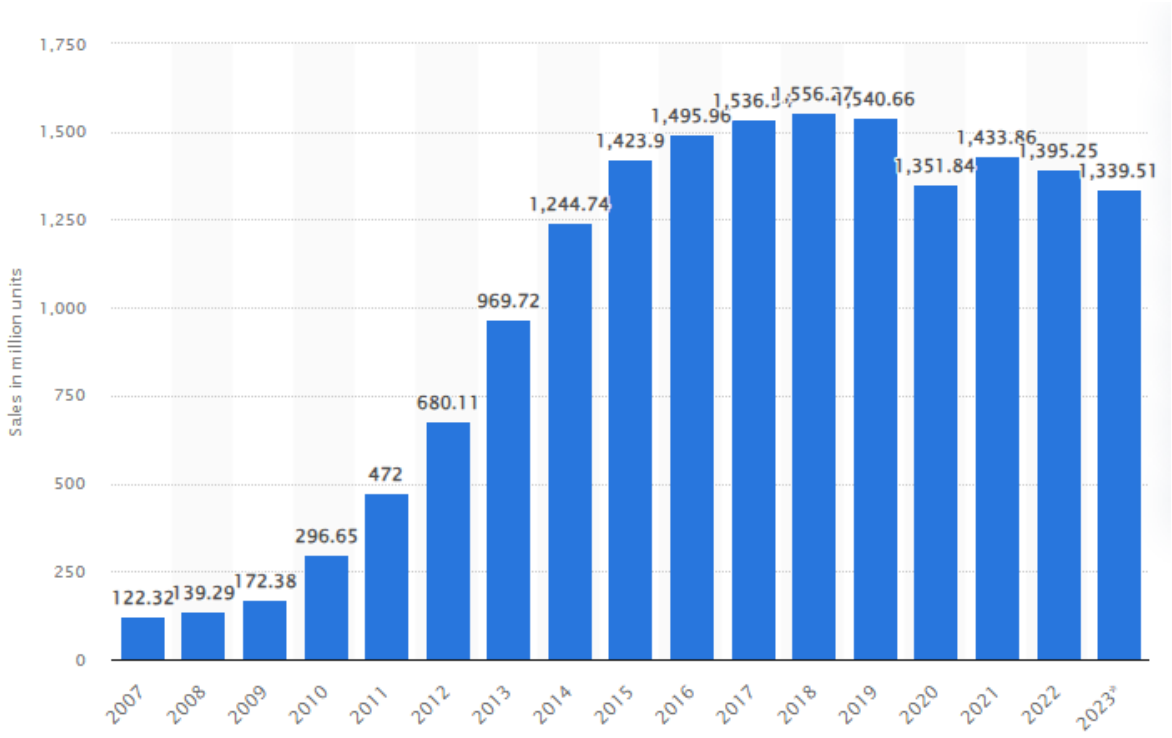

FIGURE 2.1 : Evolution annuelle du marché des smartphones

(Laricchia, 2024)

Cette croissance de l'utilisation des smartphones a ouvert de nouvelles opportunités pour les attaquants, qui ont commencé à adapter les techniques d'hameçonnage à ce nouvel environnement (Verizon, 2020). L'essor des réseaux sociaux sur mobile a également contribué à la montée de l'hameçonnage mobile où les attaquants ont commencé à exploiter ces plateformes pour créer de faux profils et diffuser des liens malveillants (Cai et al., 2020).

2.1.3 VECTEURS D'HAMEÇONNAGE MOBILE

L'hameçonnage mobile peut revêtir différentes formes. Selon le rapport de Verizon (Verizon, 2020), les cybercriminels développent constamment de nouvelles techniques pour tromper les utilisateurs et accéder à leurs informations sensibles. Ci-après les principaux vecteurs d'hameçonnage mobile :

FIGURE 2.2 : Principaux vecteurs d'hameçonnage mobile

Hameçonnage par SMS (Smishing) : les attaquants envoient des messages texte frauduleux, prétendant provenir d'institutions légitimes (Matthew, 2024), telles que des banques, des entreprises de services publics ou des organismes gouvernementaux. Ces messages incitent les utilisateurs à cliquer sur des liens malveillants ou à fournir des informations personnelles (Microsoft, 2024; OneSpan, 2024). Ce pourriel mobile est souvent un vecteur pour d'autres types d'attaques.

Hameçonnage par appel vocal (Vishing) : les cybercriminels utilisent des appels téléphoniques pour tromper les utilisateurs (Centre canadien pour la cybersécurité, 2022). Ceux-ci se passent pour des représentants d'entreprises ou de services officiels, incitant les utilisateurs à fournir des informations sensibles (Matthew, 2024).

Hameçonnage via des applications mobiles : les attaquants créent des applications mobiles malveillantes qui imitent des applications légitimes qui, une fois installées, peuvent collecter des données personnelles (Shahriar et al., 2015).

Hameçonnage sur les réseaux sociaux : les attaquants utilisent des plates-formes de médias sociaux pour créer de faux profils, utilisés par la ensuite pour envoyer des messages ou des liens malveillants aux utilisateurs (Cai et al., 2020).

Hameçonnage par le biais d'applications de messagerie instantanée : les attaquants exploitent des applications de messagerie instantanée pour envoyer des liens malveillants, des fichiers infectés ou des messages incitatifs, dans le but de voler des informations sensibles aux utilisateurs (Cai et al., 2020).

Il est important pour les utilisateurs d'être vigilants et informés sur ces différentes formes d'hameçonnage mobile afin de prendre des mesures de sécurité appropriées.

2.1.4 FACTEURS FAVORISANT L'HAMEÇONNAGE MOBILE

L'hameçonnage mobile prospère en exploitant divers facteurs qui rendent les utilisateurs plus vulnérables aux attaques. Voici quelques-uns des facteurs favorisant l'hameçonnage mobile :

Usage intensif des applications mobiles : l'utilisation fréquente d'applications mobiles pour des services en ligne telles que la banque en ligne, les achats ou les interactions sociales, crée des opportunités pour les attaquants. Les utilisateurs sont plus susceptibles de répondre à des messages ou à cliquer sur des liens qui semblent liés à ces activités.

Faiblesse des mesures de sécurité sur les appareils mobiles : comparativement aux ordinateurs, les dispositifs mobiles peuvent avoir des mesures de sécurité moins rigoureuses (Kaspersky, 2024), notamment à cause de leurs faibles capacités.

Inattention des utilisateurs : les attaques d'hameçonnage mobile utilisent souvent des tactiques d'urgence, incitant les utilisateurs à agir rapidement sans réfléchir (Goel & Jain, 2018). En effet, la

création d'un sentiment d'urgence peut conduire à des prises de décision impulsives, favorisant ainsi le succès de l'attaque.

Manque de connaissance sur les menaces : le manque de sensibilisation et de connaissance des utilisateurs sur les risques spécifiques liés à l'utilisation des appareils mobiles contribue largement à leur vulnérabilité (Centre canadien pour la cybersécurité, 2022).

Rapidité des évolutions technologiques : les avancées technologiques rapides peuvent également rendre les utilisateurs moins familiers avec les nouvelles menaces émergentes, créant ainsi des opportunités pour les attaquants d'exploiter des failles récentes (Goel & Jain, 2018).

Fonctionnalités de géolocalisation : Les applications mobiles utilisent souvent des fonctionnalités de géolocalisation. Les attaquants peuvent tirer parti de ces informations pour personnaliser les attaques et les rendre plus convaincantes en se faisant passer pour des entités locales.

Comprendre ces facteurs favorisant l'hameçonnage mobile est essentiel pour renforcer la sensibilisation des utilisateurs et mettre en place des mesures de prévention adaptées.

2.1.5 ETAPES D'UNE ATTAQUE D'HAMEÇONNAGE MOBILE

Une attaque d'hameçonnage mobile implique une planification soigneusement élaborée par les attaquants pour tromper les utilisateurs et accéder à leurs informations sensibles. D'après Proofpoint (2024), les étapes courantes d'une attaque d'hameçonnage mobile incluent :

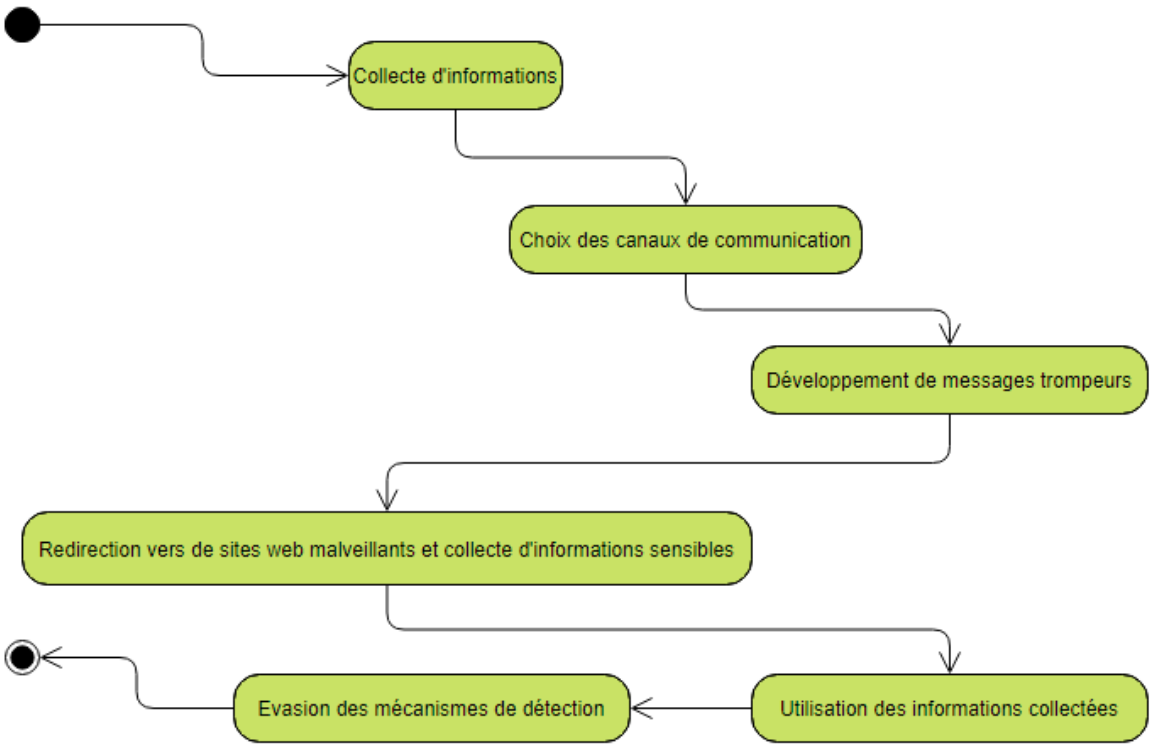

FIGURE 2.3 : Etapes d'une attaque d'hameçonnage mobile

1) Collecte d'informations : Les attaquants collectent des informations sur la cible, telles que des adresses électroniques, des numéros de téléphone, des habitudes en ligne, et d'autres détails pertinents pour personnaliser l'attaque. Les attaquants créent aussi une identité trompeuse en se faisant passer pour des entités légitimes, telles que des institutions bancaires, des services gouvernementaux, des entreprises de confiance, ou même des contacts personnels.

2) Choix des canaux de communication : Les attaquants sélectionnent les canaux de communication appropriés pour atteindre leur cible. Cela peut inclure l'envoi de SMS, de courriels, d'appels téléphoniques, ou l'utilisation de messages sur des applications de messagerie instantanée.

3) Développement de messages trompeurs : Les attaquants créent des messages frauduleux, tels que des SMS, des courriels, des messages instantanés ou des publications sur les réseaux sociaux. Ces messages sont conçus pour induire la victime en erreur, utilisant souvent des tactiques d'urgence, des offres alléchantes, ou des alertes de sécurité. Cela peut impliquer le clic

sur un lien, le téléchargement d'une application, la fourniture d'informations sensibles ou d'autres actions susceptibles de compromettre la sécurité de la victime.

4) Redirection vers des sites web malveillants et collecte d'informations sensibles : Les victimes sont redirigées vers des sites web malveillants qui imitent étroitement des sites légitimes. Une fois sur le site web malveillant, les utilisateurs sont incités à fournir des informations sensibles telles que des identifiants de connexion, des numéros de carte de crédit, des informations personnelles, ou d'autres données confidentielles.

5) Utilisation des informations collectées : Les informations sensibles collectées sont exploitées par les attaquants à des fins malveillantes, telles que le vol d'identité, la fraude financière, la vente de données collectées, ou d'autres types d'attaques.

6) Évasion des mécanismes de détection : Les attaquants utilisent ensuite diverses techniques pour échapper aux mécanismes de détection, comme le changement de numéros de téléphones d'attaque, le changement de profils de réseaux sociaux, ou l'emploi d'autres techniques pour cacher leur identité et leur localisation.

2.1.6 TYPES DE MESSAGES D'HAMEÇONNAGE MOBILE

Les messages d'hameçonnage mobile varient en forme et en contenu, mais ils partagent souvent les mêmes caractéristiques trompeuses visant à inciter les utilisateurs à prendre des décisions inappropriées. Le plus souvent les messages d'hameçonnage mobile peuvent prendre la forme de :

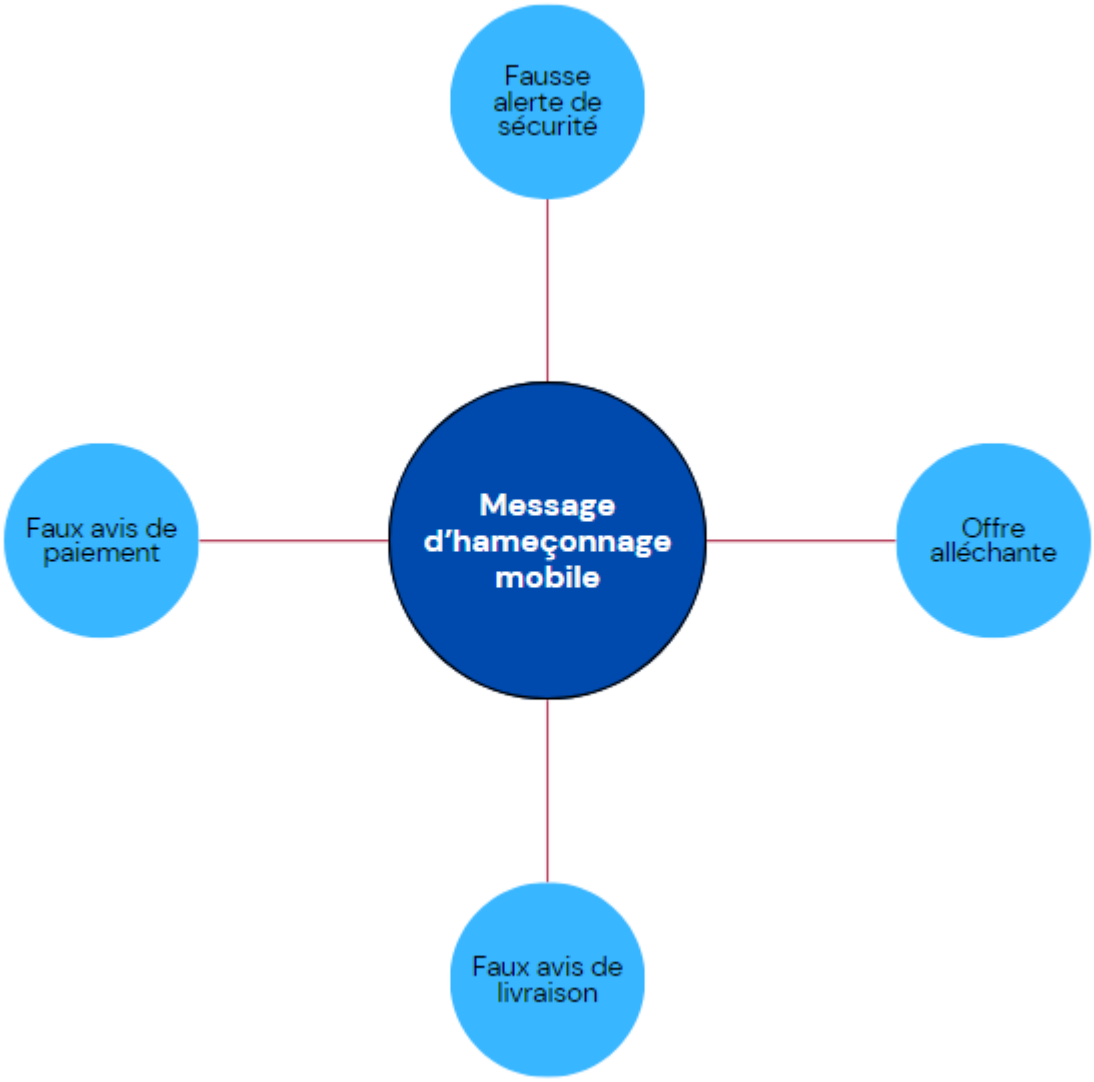

FIGURE 2.4 : Principaux types de messages d'hameçonnage mobile

Fausses alertes de sécurité : des messages prétendant provenir d'une institution légitime, telle qu'une banque ou un service en ligne, avertissent l'utilisateur d'une activité suspecte sur son compte où il est incité à cliquer sur un lien pour vérifier ses informations (Kaspersky, 2024; Proofpoint, 2024).

Offres alléchantes, faux concours, gains de loterie ou de jeux : les attaquants envoient des messages notifiant des récompenses, des offres spéciales, des gains de loterie ou des cadeaux, où l'utilisateur est invité à fournir des informations personnelles pour réclamer les récompenses ou participer (Kaspersky, 2024; Proofpoint, 2024).

Faux avis de livraison de colis : des messages prétendent informer l'utilisateur d'une livraison en attente sur une commande récente où l'utilisateur est incité à cliquer sur des liens malveillants soi-disant pour obtenir des détails ou suivre le colis (Kaspersky, 2024; Matthew, 2024).

Faux avis de facturation ou de paiement : les attaquants envoient des messages indiquant que des paiements sont dus et les utilisateurs sont incités à cliquer sur des liens pour débloquer la situation (Proofpoint, 2024).

Il est essentiel pour les utilisateurs d'être sceptiques face à de tels messages, de vérifier attentivement la légitimité des sources, d'éviter de cliquer sur des liens douteux, et de signaler tout message suspect.

2.1.7 COMMENT RECONNAITRE L'HAMEÇONNAGE MOBILE ?

Comme déjà évoqué, reconnaître une attaque d'hameçonnage mobile nécessite une vigilance constante et une compréhension des signes révélateurs de ce genre d'attaque. Selon le Centre canadien pour la cybersécurité (2022), certains critères sont à prendre en compte pour identifier une attaque d'hameçonnage mobile :

Expéditeur inconnu ou suspect : il faut être prudent si le message provient d'un expéditeur inconnu, suspect ou d'un numéro de téléphone non identifiable. Les institutions légitimes n'utilisent généralement pas de numéros de téléphone personnels pour des communications officielles.

Urgence excessive : les attaques d'hameçonnage mobile impliquent souvent des messages d'urgence exigeant une action immédiate. Il faut ainsi être vigilent face aux messages incitant à respecter une certaine échéance.

Demandes d'informations sensibles : il faut être méfiant si des gens demandent des informations sensibles telles que des mots de passe, des numéros de carte de crédit, des codes PIN, ou d'autres données personnelles. Les institutions légitimes ne sollicitent généralement pas ces informations par message ou appel.

Orthographe et grammaire déficientes : les attaques d'hameçonnage mobile peuvent contenir plusieurs erreurs grammaticales ou d'orthographe. Il faut être attentif à la qualité du langage utilisé, car les messages légitimes de grandes entreprises sont généralement bien rédigés.

Polices et graphismes incohérents : les attaquants peuvent ne pas être en mesure de reproduire fidèlement les polices et les graphismes des institutions légitimes. Il faut être attentif aux incohérences dans la présentation visuelle sur l'écran.

Liens suspects : il faut vérifier attentivement les liens dans les messages. Les attaquants utilisent des liens malveillants qui peuvent rediriger vers des sites d'hameçonnage.

Offre trop belle pour être vrai : il faut se méfier des prix gagnés dans un concours auquel on n'a jamais participé ou des prix pour lesquels il faut payer des frais.

En restant vigilant et en surveillant ces critères, les utilisateurs peuvent réduire considérablement le risque de tomber victimes d'attaques d'hameçonnage mobile.

2.1.8 EXEMPLES D'ATTAQUES PAR HAMEÇONNAGE MOBILE

Voici quelques exemples de messages d'hameçonnage mobile pour certains types d'attaques.

Fausses alertes de sécurité

Le SMS ci-après illustre une fausse alerte de sécurité

FIGURE 2.5 : Exemple d'hameçonnage mobile par une fausse alerte de sécurité

Si on analyse bien le message on peut facilement constater que le lien mentionné n'est pas le vrai site web de l'institution. De plus, après s'être entretenu avec un employé de la banque RBC nous avons été informé que l'institution ne communique jamais par SMS pour prévenir d'un problème avec une carte. C'est au client de découvrir le problème et de se rendre au guichet pour corriger ça. Par ailleurs, l'institution utilise un numéro court pour ses communications via SMS comme illustré sur l'image qui suit.

FIGURE 2.6 : Exemple de SMS pour une communication officielle de la Banque Royale

Offres alléchantes

Les messages qui suivent illustrent de telles situations

FIGURE 2.7 : Premier exemple d'hameçonnage mobile par une offre alléchante

FIGURE 2.8 : Second exemple d'hameçonnage mobile par une offre alléchante

Ici aussi on peut facilement constater qu'aucun message ne mentionne pas le vrai domaine du site web de Fido ou d'Air Canada. Par ailleurs, ces institutions communiquent officiellement par SMS avec des numéros courts comme on peut le constater sur les messages ci-après.

FIGURE 2.9 : Exemple de SMS pour une communication officielle de Fido

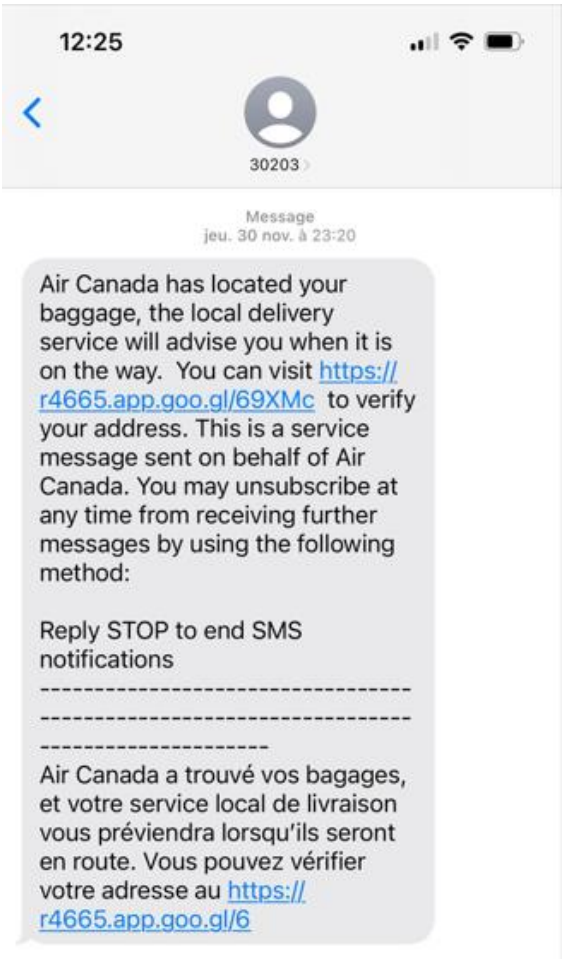

FIGURE 2.10 : Exemple de SMS pour une communication officielle d'Air Canada

Faux avis de livraison

Le message SMS suivant illustre un faux avis de livraison

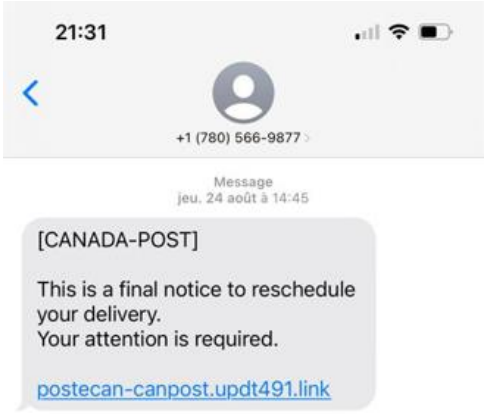

FIGURE 2.11 : Exemple d'hameçonnage mobile par un faux avis de livraison

Pour ce message également on peut constater que le nom de domaine du lien n'est pas le vrai site web de Postes Canada. Par ailleurs, après s'être entretenu avec un employé de cette institution, il nous a signalé que Postes Canada ne communique jamais par SMS car elle ne collecte pas les numéros de téléphones de ses clients. L'institution communique uniquement par courrier postal pour une notification de livraison à ses clients.

La vigilance et la prudence des utilisateurs face à de tels messages sont essentielles pour se protéger contre ces tentatives d'hameçonnage mobile.

2.1.9 ETUDE DE CAS D'UN MESSAGE D'HAMEÇONNAGE MOBILE

Etudions le message suivant pour illustrer le fonctionnement de cette menace. Celui-ci indique que le destinataire a reçu un remboursement de la part de la Société de l'Assurance Automobile du Québec (SAAQ), et se présente comme suit :

FIGURE 2.12 : Message d'hameçonnage mobile pour un remboursement de la SAAQ

L'analyse du message démontre plusieurs indices révélateurs d'une tentative d'hameçonnage mobile :

- Expéditeur suspect : Les compagnies légitimes n'utilisent généralement pas de messages textes dans leurs communications officielles avec les clients.
- Adresse URL suspecte : L'URL incluse dans le message (http://svcbservices.com) semble douteuse. Une inspection approfondie montre qu'elle n'est pas associée à la véritable société et n'est pas non plus sécurisée.
- Absence de personnalisation : Le message est générique et ne mentionne ni le nom complet du destinataire ni d'autres informations personnelles, ce qui peut également éveiller des soupçons.
- Fautes d'orthographe : Le message contient une faute d'orthographe. En effet, le déterminant qui précède le mot « surcharge » n'est pas accordé correctement.

Si on essaie de tracer là où mène cette URL, on remarque que celle-ci dirige vers une page semblable à celle d'Interac lors du transfert de fonds, mais sous le même domaine frauduleux, comme l'illustre la capture ci-dessous.

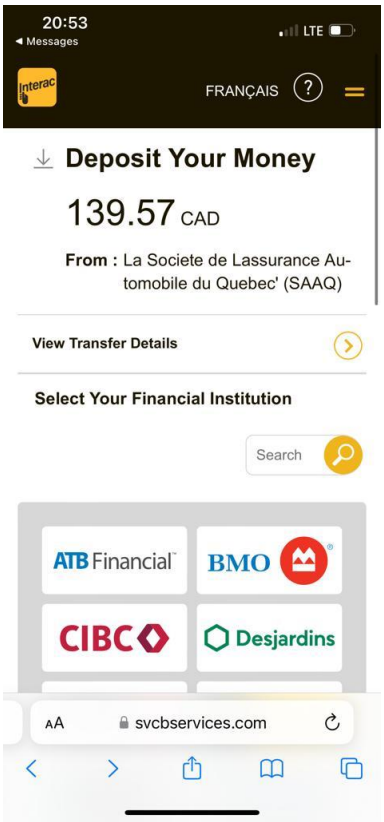

FIGURE 2.13 : Page Web d'hameçonnage imitant celle d'Interac

En cliquant sur le logo de la Royal Bank of Canada (RBC) par exemple, on est dirigé vers une page semblable à la page de connexion vers la banque en ligne de RBC, toujours sous le même domaine frauduleux.

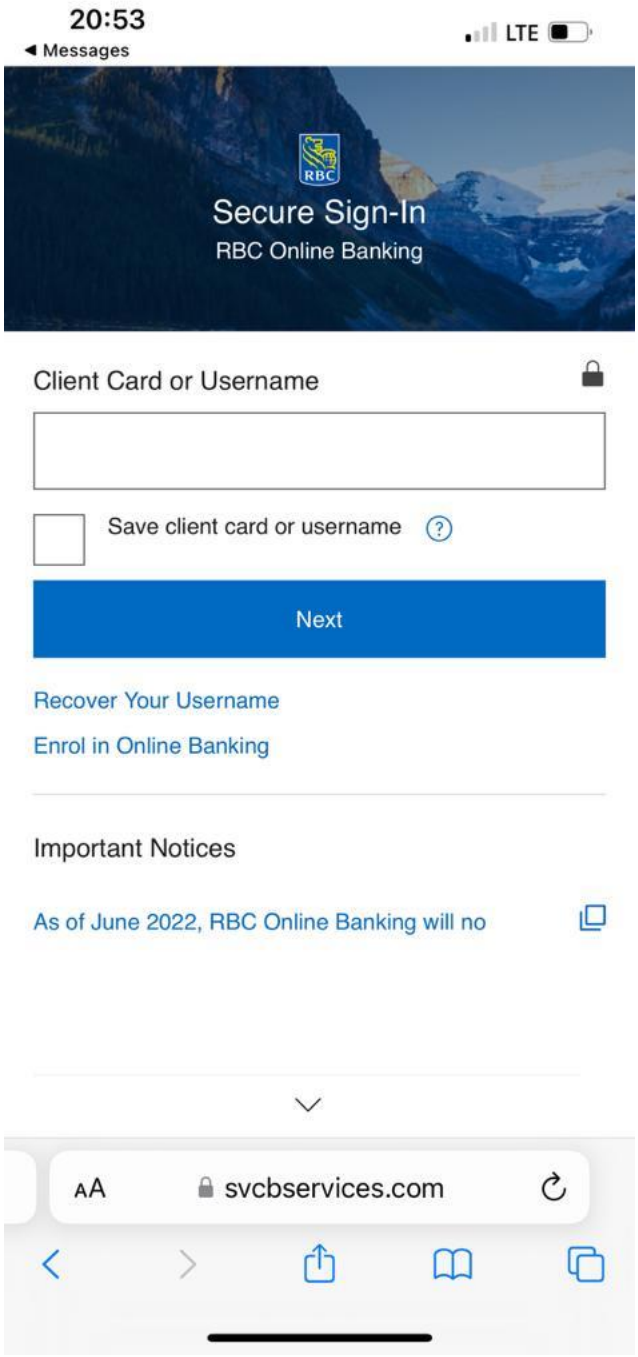

FIGURE 2.14 : Page Web d'hameçonnage imitant celle de la banque RBC

Si on ne tire pas attention et qu'on remplit les informations demandées, celles-ci seront acheminées vers l'attaquant et ce dernier pourrait avoir accès aux comptes bancaires de la victime.

De plus, une vérification de la base de données WHOIS révèle que le domaine « svcbservices.com » a été enregistré moins d'un mois avant le lancement de la tentative d'hameçonnage mobile, et a été supprimé quelques jours après.

Cet exemple démontre l'efficacité des méthodes d'analyse des messages d'hameçonnage, tout en soulignant l'importance de l'éducation des utilisateurs. Bien que la présence du logo de la SAAQ dans le message puisse le rendre convaincant à première vue, une inspection minutieuse révèle des signes clairs de fraude. Cette étude de cas illustre les dangers de l'hameçonnage mobile et l'importance de la vigilance face à ces menaces.

2.1.10 BONNES PRATIQUES POUR PREVENIR L'HAMEÇONNAGE MOBILE

Lorsqu'on est ciblé par une attaque d'hameçonnage mobile, il est essentiel de prendre des mesures immédiates pour minimiser les risques et protéger ses informations personnelles. Les actions suivantes sont recommandées (Centre canadien pour la cybersécurité, 2022 ; Kaspersky, 2024 ; Proofpoint, 2024) :

Ne pas répondre ou ne pas cliquer : il est important de ne pas répondre ni cliquer sur aucun lien quand on reçoit un message suspect. Il faut éviter d'interagir avec le message pour ne pas compromettre davantage la sécurité de ses données.

Ne fournir aucune information sensible : il ne faut jamais partager de données personnelles, d'informations financières, de mots de passe ou d'autres informations sensibles en réponse à un message suspect. Les institutions légitimes ne sollicitent généralement pas ces informations par SMS.

Signalement du message suspect : il faut signaler le message d'hameçonnage mobile à son opérateur mobile en utilisant les options de signalement disponibles. De plus, si le message prétend provenir d'une institution spécifique, il faut informer également cette institution de l'incident.

Vérification des comptes : si le message prétend provenir d'une institution financière ou d'un service en ligne, se connecter directement à son compte en utilisant les moyens sécurisés, puis vérifier les activités récentes pour s'assurer qu'aucune action non autorisée n'a été effectuée.

Scan de l'appareil pour les applications malveillantes : effectuer une analyse antivirus sur l'appareil mobile pour rechercher la présence éventuelle d'applications malveillantes. Il faut veiller à utiliser une solution de sécurité mobile fiable pour renforcer la protection de son appareil.

Mise à jour des applications et du système : s'assurer que toutes les applications et le système d'exploitation de l'appareil mobile sont à jour. En effet, les mises à jour peuvent contenir des correctifs de sécurité pour les vulnérabilités connues.

Si on a fourni des informations sensibles ou si l'on suspecte une atteinte à la sécurité de ses comptes, il faut contacter immédiatement les institutions concernées pour les informer de la situation. Ils pourront prendre des mesures supplémentaires pour protéger les comptes et donner d'autres directives.

2.1.11 MESURES DE PREVENTION MISES EN PLACE PAR LES INTERVENANTS

Les opérateurs de téléphonie, les éditeurs d'applications et les éditeurs de systèmes d'exploitation mobiles mettent en place divers moyens pour contrer l'hameçonnage mobile et renforcer la sécurité des utilisateurs. En voici quelques-uns :

Filtrage de SMS malveillants : certains systèmes d'exploitation intègrent des mécanismes de filtrage automatique pour identifier les SMS malveillants, réduisant ainsi l'impact de l'hameçonnage mobile (Matthew, 2024).

Base de données de numéros malveillants : les opérateurs maintiennent des bases de données de numéros de téléphone suspects, signalant les utilisateurs lorsque des SMS ou des appels proviennent de sources potentiellement malveillantes.

Signalement de numéros malveillants : les opérateurs de téléphonie et d'autres entités offrent aux utilisateurs les options de signalement de numéros de téléphone ou de messages suspects, contribuant ainsi à l'amélioration des bases de données de filtrage.

Mises à jour de sécurité : Les éditeurs publient régulièrement des mises à jour de sécurité qui incluent des correctifs de sécurité pour les vulnérabilités liées à l'hameçonnage mobile.

Alertes d'hameçonnage : Les éditeurs peuvent intégrer des alertes de sécurité pour informer les utilisateurs des risques liés aux messages ou appels reçus.

Il est important pour les utilisateurs de maintenir leurs systèmes d'exploitation et applications à jour, d'être conscients des autorisations demandées par les applications, et de suivre les bonnes pratiques de sécurité pour réduire les risques d'hameçonnage mobile.

2.1.12 CONCLUSION

L'attaque contre AOL a démontré la vulnérabilité des utilisateurs face à des tactiques d'ingénierie sociale sophistiquées. Les cybercriminels ont réussi à exploiter la confiance des utilisateurs en imitant fidèlement l'apparence des communications officielles de la plateforme, incitant ainsi de nombreux utilisateurs à divulguer leurs informations personnelles.

De nos jours, les attaques sont devenues plus sophistiquées, ciblées et difficiles à détecter (Pensez cybersécurité, 2021), illustrant la nécessité constante de mesures de prévention et de sensibilisation pour contrer cette menace persistante. En effet, il est essentiel pour les utilisateurs de rester informés sur les techniques d'hameçonnage mobile et d'adopter des pratiques de sécurité pour se protéger contre ces attaques. Ces pratiques incluent notamment la vérification des sources, la méfiance à l'égard des messages d'urgence, et l'utilisation de solutions de sécurité mobile. La sensibilisation et l'éducation continue sur les risques associés à l'hameçonnage mobile sont donc cruciales pour renforcer la résilience des utilisateurs face à cette menace persistante, et les jeux sérieux s'avèrent être un moyen efficace.

2.2 LES JEUX SERIEUX

2.2.1 DEFINITION ET CARACTERISTIQUES DES JEUX SERIEUX

Les jeux sérieux (« serious games », en anglais) représentent une catégorie de jeux vidéo développés non seulement pour divertir, mais aussi pour éduquer, former, ou sensibiliser les utilisateurs à des sujets spécifiques tels que l'éducation, la santé, la formation professionnelle ou la sensibilisation à la sécurité (Hocine et al., 2011). Mostafa & Faragallah (2019) y va dans le même sens en mentionnant qu'un jeu sérieux se distingue d'un jeu traditionnel par sa finalité, qui est d'atteindre un objectif utilitaire en plus du divertissement. Ainsi, les jeux sérieux exploitent la dynamique de jeu pour motiver les utilisateurs à s'engager activement avec le contenu éducatif, facilitant ainsi l'acquisition de nouvelles compétences ou connaissances.

2.2.2 LES JEUX SERIEUX DANS L'EDUCATION ET LA SENSIBILISATION

Dans le domaine éducatif, les jeux sérieux sont largement utilisés pour rendre l'apprentissage plus interactif et engageant. Des recherches ont prouvé que les jeux sérieux peuvent améliorer la rétention de l'information, favoriser l'apprentissage par la pratique, et stimuler la motivation des apprenants (Mostafa & Faragallah, 2019). À titre d'exemple, des jeux comme Duolingo pour l'apprentissage des langues ou SimCity pour l'enseignement de la planification urbaine démontrent comment des concepts complexes peuvent être enseignés de manière ludique.

Les jeux sérieux sont également devenus des outils précieux dans la sensibilisation à la sécurité, notamment dans le domaine de la cybersécurité (Mostafa & Faragallah, 2019). Comme nous allons le voir dans la section sur les travaux connexes, des jeux sérieux ont déjà été développés pour sensibiliser les utilisateurs aux menaces de sécurité en ligne. Ces jeux mettent l'accent sur la compréhension des mécanismes des attaques et les stratégies de défense à travers des simulations interactives.

2.2.3 LES JEUX SERIEUX ET LA CYBERSECURITE

Le domaine de la cybersécurité a vu un intérêt croissant pour les jeux sérieux, en raison de leur potentiel à simuler des scénarios d'attaques réelles et à éduquer les utilisateurs sur les bonnes pratiques de sécurité (Onashoga et al., 2019). Plus particulièrement, les jeux sérieux sont utilisés pour enseigner la détection de menaces, comme l'hameçonnage, où les utilisateurs peuvent apprendre à reconnaître les signes d'une attaque dans un environnement contrôlé mais réaliste.

2.2.4 LES JEUX SERIEUX POUR LA SENSIBILISATION A L'HAMEÇONNAGE MOBILE

Comme déjà évoqué dans les sections précédentes, l'évolution rapide de l'hameçonnage, particulièrement avec la montée en puissance des plateformes mobiles, a créé un besoin croissant de sensibilisation adaptée à ces nouveaux vecteurs de menace. Les jeux sérieux conçus spécifiquement pour la sensibilisation à l'hameçonnage mobile peuvent jouer un rôle crucial dans la formation des utilisateurs à identifier et à éviter certaines attaques. La capacité à reproduire les scénarios typiques auxquels les utilisateurs sont confrontés sur leurs appareils mobiles (Onashoga et al., 2019) justifie l'intérêt de développement d'un jeu sérieux pour la sensibilisation à l'hameçonnage mobile. Ce type de jeu peut intégrer des messages textuels simulés, des appels téléphoniques, et des notifications, offrant ainsi une expérience d'apprentissage immersive. En simulant ces scénarios, les utilisateurs peuvent apprendre à reconnaître les signes d'hameçonnage dans un environnement sans risque, améliorant ainsi leur vigilance dans des situations réelles.

2.3 TRAVAUX CONNEXES

Plusieurs études se sont penchées sur la création de jeux sérieux pour la sensibilisation à la cybersécurité. Les paragraphes suivants explorent d'importantes initiatives de jeux éducatifs développées pour alerter les utilisateurs sur les menaces d'ingénierie sociale, notamment l'hameçonnage.

SEAG (Social Engineering Awareness Game) est un jeu développé avec Construct2 pour sensibiliser les utilisateurs aux différents types d'attaques d'ingénierie sociale (Olanrewaju & Zakaria, 2015). Le jeu possède trois niveaux : les deux premiers se concentrent sur les concepts de

base et le dernier présente des scénarios concrets d'ingénierie sociale. Les points sont attribués en fonction des réponses du joueur. Le jeu a été évalué par une comparaison de 2 types de tests, une version papier ainsi qu'une session avec le jeu développé, auprès de 20 étudiants. Les résultats de la session ludique ont montré la meilleure moyenne. Cette approche d'évaluation confirme une fois de plus l'efficacité des jeux sérieux pour la sensibilisation à la cybersécurité.

Muhly et al. (2022) ont développé un jeu de cartes visant la sensibilisation à des multiples attaques d'ingénierie sociale. Les joueurs incarnent des attaquants et exploitent les failles de sécurité potentielles du réseau d'une entreprise. Les attaques sont exécutées à l'aide de cartes, et des points sont attribués en fonction de la gravité de l'attaque formulée. Le jeu a été évalué au moyen d'observations et d'entretiens auprès de 97 participants. Les résultats ont montré qu'avec quelques modifications, le jeu présente un potentiel comme outil de sensibilisation à l'ingénierie sociale. Une approche d'évaluation par une session de jeu, prenant en compte la progression du score, aurait pu fournir davantage d'informations sur la pertinence du jeu sérieux.

Playing Safe (Newbould & Furnell, 2009) est un jeu visant à sensibiliser le public aux différents types d'attaques d'ingénierie sociale, dont l'hameçonnage. Le jeu propose des questions à choix multiples, et des points sont attribués en fonction des réponses du joueur. Le jeu sérieux a été évalué au moyen d'une session de jeu et de questionnaires, auprès de 21 participants. Les résultats ont montré qu'aucun participant n'a obtenu un score inférieur à 55 % pendant la session de jeu, et que 86 % des participants estimaient avoir amélioré leurs connaissances.

Securix (Onashoga et al., 2019) est un jeu 3D sur ordinateur, développé avec Unity, pour sensibiliser aux attaques d'hameçonnage. Il propose deux niveaux, débutant et avancé, chacun se focalisant sur trois catégories d'attaques : les URL, les courriels et les sites web. Le jeu présente des scénarios d'URL, de courriels et de sites web, et les joueurs doivent déterminer s'ils sont légitimes ou frauduleux. Des points sont attribués ou déduits en fonction des réponses des joueurs. Le jeu a été évalué à l'aide de questionnaires auprès de 50 participants. 95 % d'entre eux ont déclaré que le jeu était pertinent pour la sensibilisation.

RansomAware (Butt, 2023) est un jeu destiné aux environnements Android et PC, développé avec la plateforme MIT App Inventor. Il vise à sensibiliser les joueurs aux attaques d'hameçonnage. Il présente aux joueurs des scénarios de courriels qu'ils doivent accepter ou refuser selon qu'ils sont légitimes ou malveillants. Des points sont attribués en conséquence. L'évaluation du jeu a été réalisée à l'aide de questionnaires et d'entretiens semi-structurés auprès de 30 participants. Les résultats ont montré que le jeu était pertinent pour sensibiliser à l'hameçonnage.

Phish Phinder (Misra et al., 2017) est un jeu mobile conçu pour sensibiliser le public aux courriels et URLs d'hameçonnage. Les points sont attribués en fonction des réponses fournies. L'évaluation du jeu n'a pas été réalisée.

Gamagedara Arachchilage (2012) a développé un jeu mobile en utilisant l'émulateur MIT App Inventor, afin de sensibiliser le public aux URLs d'hameçonnage. L'évaluation du jeu a été réalisée à l'aide de tests utilisateurs et de questionnaires auprès de 20 participants. L'étude a révélé que les participants ayant joué au jeu mobile étaient plus capables d'identifier les sites web frauduleux, par rapport à ceux ayant consulté ces sites sans formation, avec une amélioration de 29 %. Cette approche d'évaluation donne plus de précision sur l'efficacité du jeu sérieux.

PhishI (Fatima et al., 2019) est un jeu conçu pour sensibiliser les utilisateurs aux courriels d'hameçonnage. Le joueur incarne un attaquant. L'attaque se déroule en quatre phases d'une durée d'au moins 15 minutes chacune. Le jeu a été évalué par des tests utilisateurs, des questionnaires et des observations, sur 63 participants. L'étude a conclu que les résultats globaux de l'évaluation du jeu étaient pertinents.

Bird's Life (Weanquoi et al., 2018) est un jeu 2D développé avec Unity, pour sensibiliser le public aux courriels d'hameçonnage. Déployable sur ordinateur, sur le Web et sur les plateformes mobiles, il comporte trois niveaux. Le jeu a été évalué par des tests utilisateurs et des questionnaires auprès de 30 étudiants. L'étude a révélé que les participants ayant joué au jeu mobile étaient plus capables d'identifier les courriels frauduleux, par rapport à ceux ayant consulté les sites web sans formation, avec une amélioration moyenne de 37,5 %.

Les résultats de ces jeux sérieux indiquent qu'ils peuvent significativement améliorer la capacité des utilisateurs à reconnaître et à éviter les attaques d'hameçonnage. Cependant, peu d'entre eux se concentrent exclusivement sur l'hameçonnage mobile, laissant un vide dans la recherche et le développement d'outils spécifiquement conçus pour ce contexte. *SafeMobile Adventure*, en tant que jeu sérieux pour la sensibilisation à l'hameçonnage mobile, vise à combler cette lacune en adaptant ses scénarios de jeu et ses outils pédagogiques aux défis uniques des utilisateurs de smartphones.

2.4 CONCLUSION

La revue de la littérature présentée dans ce chapitre met en lumière les enjeux majeurs et les lacunes actuelles dans la sensibilisation contre l'hameçonnage mobile. L'analyse de l'hameçonnage mobile a montré que cette forme de cyberattaque est en pleine expansion, exploitant les spécificités des plateformes mobiles pour tromper les utilisateurs. Les vulnérabilités des systèmes et le manque de vigilance des utilisateurs mobiles en font une cible de choix pour les cybercriminels. Les travaux précédents montrent que les jeux sérieux constituent une approche efficace pour la sensibilisation aux cybermenaces, mais qu'il reste encore un potentiel inexploité dans le domaine de l'hameçonnage mobile. Cela ouvre la voie à de nouveaux travaux dans la conception de jeux spécifiques à cette forme d'hameçonnage, comme celui développé dans le cadre de ce travail.

CHAPITRE III

ANALYSE DES BESOINS ET CONCEPTION DU JEU

Le développement d'un jeu sérieux nécessite une compréhension approfondie des besoins des utilisateurs ainsi qu'une conception minutieuse pour garantir l'efficacité pédagogique et l'engagement.

3.1 ANALYSE DES BESOINS

L’analyse des besoins a constitué une étape fondamentale dans le processus de développement du jeu sérieux, en assurant sa pertinence pédagogique et son attractivité auprès des utilisateurs finaux. Cette phase a permis d’identifier les exigences éducatives, fonctionnelles et techniques du public cible, tout en les alignant avec les objectifs de sensibilisation à la cybersécurité mobile.

3.1.1 EXIGENCES PEDAGOGIQUES

L’objectif principal sur le plan éducatif consistait à doter les utilisateurs de la capacité à identifier avec précision les tentatives d’hameçonnage sur appareils mobiles et à y réagir de manière appropriée. Il s’agissait notamment de sensibiliser aux techniques d’hameçonnage fréquemment rencontrées (notifications frauduleuses de livraison, fausses alertes de suspension de compte, fausses annonces de gains) et de développer des compétences d’analyse critique pour évaluer les messages suspects. À cette fin, le jeu devait intégrer des scénarios réalistes inspirés de cas concrets d’hameçonnage mobile.

3.1.2 EXIGENCES DES UTILISATEURS

Le public visé regroupait des utilisateurs de smartphones aux profils variés, incluant tant des novices que des personnes disposant d’une expérience préalable en cybersécurité. Il en découlait une nécessité d’accessibilité, d’intuitivité et d’adaptation du contenu aux différents

niveaux de connaissance. Par ailleurs, les parties prenantes, notamment les formateurs et chercheurs en cybersécurité, ont souligné l'importance de disposer de mécanismes de sauvegarde de données, permettant d'évaluer l'impact du jeu sur les apprentissages des utilisateurs.

3.1.3 EXIGENCES FONCTIONNELLES

Les fonctionnalités essentielles identifiées comprenaient :

- Une présentation aléatoire de messages légitimes et frauduleux ;
- Un système de décision permettant à l'utilisateur de classifier chaque message comme « légitime » ou « hameçonnage » ;
- Un retour immédiat et explicatif pour chaque choix effectué ;
- Un système de suivi des réponses correctes et erronées à des fins d'analyse ;
- Une interface ergonomique, spécifiquement optimisée pour les écrans de terminaux mobiles.

3.1.4 EXIGENCES TECHNIQUES

Le jeu a été développé à l'aide de la plateforme Construct 3, en vue d'une compatibilité optimale avec les dispositifs mobiles. L'ensemble des ressources multimédias (images et sons) a été adapté aux contraintes de performance sur mobile, et la possibilité d'un fonctionnement hors connexion a été envisagée afin de limiter la dépendance à l'accès réseau.

En définitive, cette phase d'analyse a permis de poser les fondations méthodologiques nécessaires pour orienter la conception et le développement du jeu, en veillant à ce que les objectifs pédagogiques et les exigences d'utilisation soient pleinement satisfaits.

3.2 OBJECTIFS PEDAGOGIQUES DU JEU

Le jeu sérieux développé a pour objectif principal de sensibiliser les utilisateurs aux dangers de l'hameçonnage mobile et de leur enseigner à reconnaître et à réagir correctement face à ces menaces. Les objectifs pédagogiques spécifiques visent à :

- Fournir une compréhension approfondie des techniques utilisées par les attaquants.
- Enseigner aux utilisateurs à reconnaître les signes d'un message d'hameçonnage mobile tels que les éléments suspects dans les SMS ou dans les messages sur les applications de messagerie instantanée.
- Familiariser les utilisateurs avec les meilleures pratiques de sécurité mobile telles que l'analyse des messages, la vérification des URLs contenus dans le message ou l'expéditeur de celui-ci.
- Renforcer les compétences des utilisateurs en matière de gestion des risques, en les aidant à évaluer les menaces potentielles et à prendre des décisions éclairées pour protéger leurs informations personnelles.
- Promouvoir une bonne défense en encourageant les comportements sécurisés telle que la prudence lors de l'utilisation d'applications mobiles.
- Évaluer les connaissances et les compétences des utilisateurs par le biais de tests intégrés au jeu sérieux.

Ces objectifs pédagogiques ont pour but de former les utilisateurs à reconnaître et à contrer les menaces d'hameçonnage mobile, renforçant ainsi leur sécurité et leur confiance dans l'utilisation des appareils mobiles.

3.3 APPROCHE METHODOLOGIQUE DE DEVELOPPEMENT

Le développement du jeu sérieux a nécessité une approche méthodologique rigoureuse et flexible. Cette section présente la méthode adoptée pour concevoir, développer, et tester le jeu, en mettant l'accent sur l'utilisation combinée de la méthode Agile et du Design Thinking. Ces deux méthodes ont été choisies pour leur capacité à s'adapter aux besoins des utilisateurs.

3.3.1 LA METHODE AGILE

3.3.1.1 DEFINITION ET PRINCIPES DE BASE

La méthode Agile est une approche de gestion de projet centrée sur l'itération rapide et la flexibilité. Badreau (2021) et Abrahamsson et al. (2017) soulignent que, contrairement aux méthodes traditionnelles en cascade ou en V, Agile favorise des cycles de développement courts appelés Sprints, au cours desquels des fonctionnalités spécifiques sont conçues, développées, testées, et améliorées en fonction des retours d'expérience. Les principes fondamentaux de l'Agile incluent donc la collaboration avec les parties prenantes, l'adaptation aux changements, la livraison fréquente de petites portions de produit, et l'amélioration continue. La figure suivante illustre les phases de la méthode Agile :

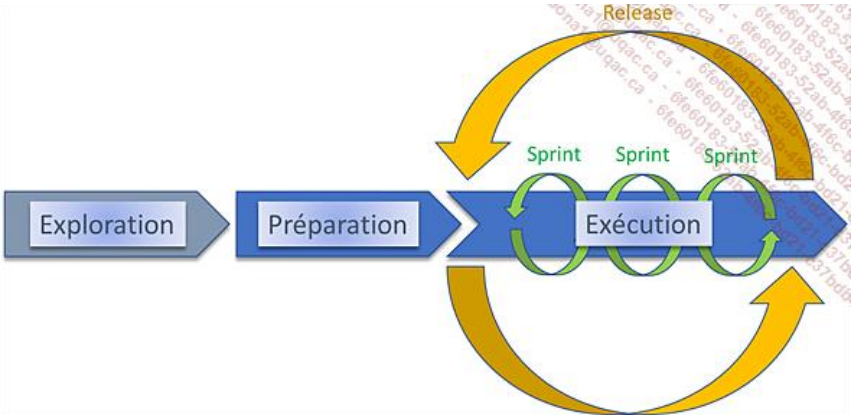

FIGURE 3.1 : Phases de la méthode Agile

(Badreau, 2021)

3.3.1.2 POURQUOI AGILE ?

Dans le cadre du développement d'un jeu sérieux, la méthode Agile est particulièrement adaptée en raison de sa capacité à gérer les incertitudes et à s'ajuster aux retours utilisateurs. Le processus de création de ce jeu nécessite une forte réactivité pour intégrer les suggestions des testeurs, affiner les mécaniques de jeu, et optimiser l'expérience utilisateur. Pour ce fait, le gameplay imaginé au départ a été modifié afin d'augmenter l'interaction du joueur avec le jeu et par conséquent améliorer la motivation. Agile permet également une meilleure gestion des priorités, en

s'assurant que les fonctionnalités essentielles sont développées en premier et que le jeu peut être testé et validé tout au long du processus.

3.3.1.3 APPLICATION DE LA METHODE AGILE

Le développement du jeu s'est déroulé en plusieurs Sprints, chacun d'une durée de deux à trois semaines. Chaque Sprint avait des objectifs spécifiques, tels que la conception et l'intégration des scénarios d'hameçonnage, l'intégration des mécanismes de feedback, ou l'amélioration de l'interface utilisateur. À la fin de chaque Sprint, des tests utilisateurs ont été effectués, permettant d'apporter des ajustements immédiats avant de passer au Sprint suivant. Ce processus a permis de maintenir une progression continue tout en assurant la qualité du produit final.

3.3.2 LE DESIGN THINKING

3.3.2.1 DEFINITION ET ETAPES CLES

Meinel et al. (2011) définit le Design Thinking comme une approche centrée sur l'utilisateur, visant à résoudre des problèmes complexes par l'innovation et la créativité. Il se décompose en cinq étapes :

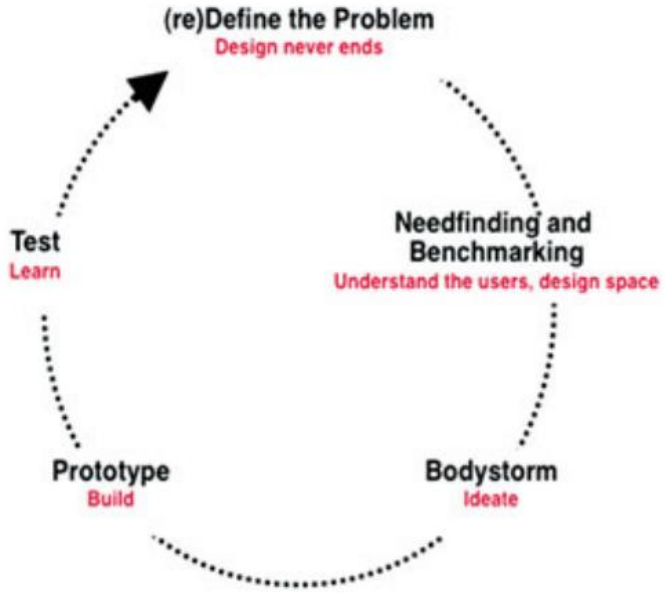

FIGURE 3.2 : Phases du Design Thinking

(Meinel et al., 2011)

Cette méthode commence donc par une compréhension profonde des besoins et des comportements des utilisateurs finaux, suivie par une phase de brainstorming pour générer des solutions créatives. Les prototypes sont ensuite rapidement développés et testés pour évaluer leur efficacité avant d'être améliorés ou modifiés.

3.3.2.2 INTEGRATION DU DESIGN THINKING DANS LE DEVELOPPEMENT DU JEU

L'intégration du Design Thinking dans le développement de ce jeu sérieux a permis de créer un produit qui répond véritablement aux besoins des utilisateurs en matière de sensibilisation à l'hameçonnage mobile. La phase d'empathie (compréhension des besoins des utilisateurs) a impliqué des observations pour comprendre comment les utilisateurs interagissent avec leurs appareils mobiles et quels types de messages d'hameçonnage ils rencontrent. Sur cette base, des scénarios de jeu ont été conçus pour reproduire ces situations dans un environnement contrôlé. La phase de prototypage a permis de développer rapidement des versions simplifiées du jeu, qui ont été testées avec un groupe restreint d'utilisateurs pour recueillir des feedbacks et affiner le produit.

3.3.3 COMBINAISON DES METHODES AGILE ET DESIGN THINKING

3.3.3.1 COMPLEMENTARITE DES METHODES

La combinaison des méthodes Agile et Design Thinking a offert un cadre de développement robuste et adaptable. Le Design Thinking a permis de bien définir les besoins des utilisateurs et de générer des idées créatives pour y répondre, tandis que l'Agile a fourni une structure pour itérer rapidement et intégrer les feedbacks. Cette complémentarité a permis de maintenir un focus constant sur les utilisateurs tout en garantissant que le développement progressait de manière efficace et contrôlée.

3.3.3.2 APPLICATION PRATIQUE DANS LE PROJET

Dans la pratique, le projet a suivi un cycle de développement itératif où chaque Sprint Agile commençait par une session d'idéation basée sur les principes du Design Thinking. Les prototypes développés pendant les Sprints étaient testés en fin de cycle, et les retours d'expérience étaient

utilisés pour améliorer ces prototypes et planifier le Sprint suivant. Cette approche a permis de créer un jeu sérieux non seulement fonctionnel, mais aussi étroitement aligné avec les objectifs pédagogiques de sensibilisation à l'hameçonnage mobile. Le schéma ci-dessous illustre la méthodologie suivie :

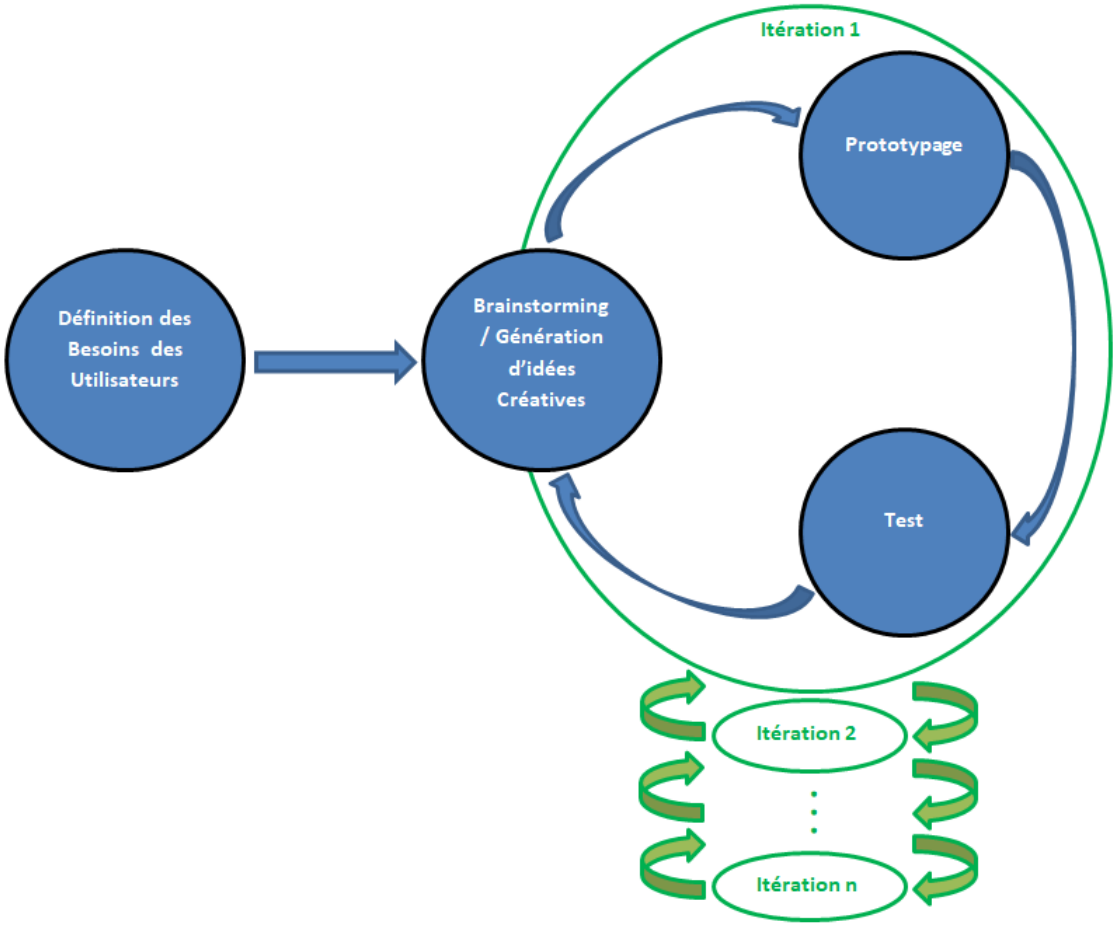

FIGURE 3.3 : Méthodologie de développement combinant Agile et Design Thinking

(Irambona et al., 2025)

3.4 CONCEPTION DU JEU

Le processus de conception du jeu sérieux repose sur une approche centrée sur l'utilisateur et a été structuré en plusieurs phases, allant de la conceptualisation initiale aux détails de la mise en œuvre.

3.4.1 STRUCTURE ET SCENARISATION

Le jeu est structuré en 2 niveaux de difficulté croissante. Chaque niveau présente des scénarios réalistes de messages basés sur des exemples réels de messages d'hameçonnage. Les scénarios sont choisis dans le jeu de façon aléatoire dans un bassin de 48 messages, dont 30 (±60%) représentent des messages d'hameçonnage et 18 (±40%) des messages légitimes. Ceci permet aux utilisateurs de ne pas mémoriser le jeu, et par conséquent, de développer progressivement leurs compétences en matière de détection et de réaction.

Les utilisateurs naviguent dans des environnements simulés où ils doivent résoudre des quizz sous forme de messages. Ils doivent analyser ces messages, identifier ceux qui sont suspects et ceux qui ne le sont pas, et prendre les actions appropriées. Des feedbacks immédiats sont fournis pour chaque décision, renforçant ainsi l'apprentissage.

3.4.2 MECANIQUES DE JEU ET FEEDBACK

Les mécaniques de jeu sont centrées sur l'interaction utilisateur et le renforcement des comportements sécuritaires. Chaque scénario est conçu pour être immersif, avec des choix et des feedbacks pour chaque action entreprise par l'utilisateur.

Le système de feedback est une composante clé, offrant des retours détaillés sur les choix faits par l'utilisateur. Ainsi, si l'utilisateur identifie correctement un message d'hameçonnage, il reçoit une explication sur les indices qui ont révélé la tentative de fraude. En cas d'erreur, le feedback souligne les signaux manqués et explique la bonne démarche à suivre.

3.4.3 INTERFACE UTILISATEUR

L'interface utilisateur (UI) a été conçue pour être intuitive et proche de l'expérience d'utilisation d'un smartphone. Cela inclut des éléments familiers tels que les icônes de messages et les menus de navigation, afin de minimiser la courbe d'apprentissage et de maximiser l'immersion. L'UI joue un rôle crucial dans l'engagement de l'utilisateur, facilitant la navigation tout en rendant l'expérience de jeu agréable et informative.

3.5 PROTOTYPAGE ET TEST UTILISATEUR

Une fois la conception initiale réalisée, un prototype du jeu a été développé et testé avec un groupe restreint d'utilisateurs. Ces tests ont permis de recueillir des retours précieux sur l'expérience utilisateur, la difficulté des scénarios, et l'efficacité des feedbacks. Les ajustements nécessaires ont été faits pour améliorer la jouabilité et assurer que les objectifs pédagogiques soient atteints de manière optimale.

3.6 CONCLUSION

Ce chapitre a détaillé l'analyse des besoins des utilisateurs et la conception du jeu sérieux pour la sensibilisation à l'hameçonnage mobile. En mettant l'accent sur une approche centrée sur l'utilisateur et en intégrant des mécaniques de jeu efficaces, le jeu est conçu pour offrir une expérience engageante et éducative, capable de former les utilisateurs à identifier et réagir face aux menaces d'hameçonnage mobile. Les prochaines étapes du projet se concentreront sur l'implémentation complète du jeu, suivie de son évaluation pour mesurer l'atteinte des objectifs pédagogiques.

CHAPITRE IV

DEVELOPPEMENT DU JEU

Le développement du prototype de jeu sérieux constitue une étape cruciale dans la réalisation de ce projet. Ce chapitre décrit en détail le processus de développement du jeu *SafeMobile Adventure*, y compris les outils et technologies utilisés, les phases de création du prototype, et les défis rencontrés. L'objectif est de produire un prototype fonctionnel qui incarne les concepts de design préalablement établis et qui puisse être testé pour évaluer son efficacité pédagogique.

4.1 OBJECTIFS DE DEVELOPPEMENT

Le développement du prototype a pour objectifs principaux de :

- **Valider les concepts de design :** Tester les scénarios de jeu, les mécaniques, et l'interface utilisateur.
- **Évaluer l'expérience utilisateur :** Assurer que le jeu est engageant, intuitif, et efficace pour atteindre les objectifs pédagogiques de sensibilisation à l'hameçonnage mobile.
- **Identifier et résoudre les problèmes techniques :** Repérer les bugs, les incohérences, et les limitations technologiques avant de passer à la phase de développement final.

4.2 TECHNOLOGIES ET OUTILS UTILISES

Pour le développement du prototype, plusieurs technologies et outils ont été sélectionnés en fonction des besoins spécifiques du projet et de la nécessité de prototyper rapidement.

4.2.1 MOTEUR DE JEU ET BASE DE DONNEES

Construct 3 a été choisi comme moteur de jeu en raison de sa polyvalence, de sa large communauté, et de sa capacité à déployer des jeux sur diverses plateformes mobiles. Les fonctionnalités de Construct 3, telles que les comportements préconfigurés et les événements

déclencheurs, ont facilité l'élaboration rapide du gameplay et des interactions utilisateur-jeu, tout en offrant une grande flexibilité pour ajuster et améliorer le prototype tout au long du développement.

Google Sheets a été choisi comme base de données pour sauvegarder en ligne les données de performance du joueur dans le jeu. Cet outil a été adopté pour faciliter les processus d'exportation de la base de données et de traitement des données de performance via un logiciel de tableur.

4.2.2 OUTILS DE CONCEPTION GRAPHIQUE

Les effets visuels du jeu ont été récupérés sur le site Web « https://pngtree.com », tandis que les messages d'hameçonnage ont presque tous été récupérés auprès des téléphones des utilisateurs. Une très petite portion de messages a été récupérée en ligne sur les sites Web de certaines organisations gouvernementales du Canada, pour compléter les catégories de messages d'hameçonnage moins représentées. Ces images ont ensuite été traitées avec les logiciels PhotoPA et Paint pour les adapter aux besoins du jeu. PhotoPA est un éditeur d'image en ligne qui se distingue par son interface proche de Photoshop, tout en étant accessible directement via un navigateur. Cet outil a été utilisé pour les modifications avancées des images, telles que la création de textures, le redimensionnement des éléments graphiques, et la gestion des calques. En complément, Paint, un logiciel plus simple et léger, a servi à des retouches mineures et rapides des images, telles que le recadrage ou la modification de petites zones graphiques. Ces deux outils combinés ont permis d'optimiser le processus de conception graphique tout en garantissant la cohérence visuelle du jeu.

4.2.3 ELEMENTS SONORES

Les éléments sonores utilisés dans le jeu, tels que les effets sonores et les musiques d'ambiance, ont été récupérés à partir de deux plateformes en ligne gratuites : Pixabay et Itch.io. Pixabay (https://pixabay.com) est une banque de ressources libres de droits qui offre une large gamme de contenus multimédia, y compris des effets sonores et des musiques. Cette plateforme a été principalement utilisée pour obtenir les effets sonores. Le site Web Itch.io

(https://sfbgames.itch.io), quant à lui, est une plateforme dédiée aux créateurs de jeux indépendants, proposant des assets sonores gratuits ou payants. La plateforme a été principalement utilisée pour obtenir des musiques d'ambiance.

4.3 PHASES DE DEVELOPPEMENT

Le développement du prototype s'est déroulé en plusieurs phases, chacune avec des objectifs spécifiques :

4.3.1 PHASE 1 : PREPARATION ET PLANIFICATION

La première phase consistait à planifier le développement du prototype. Cela incluait la définition des fonctionnalités essentielles à inclure, l'établissement du calendrier de développement, et l'allocation des ressources nécessaires. Une liste des fonctionnalités et des tâches a été créé, priorisant les éléments critiques tels que les scénarios de messages d'hameçonnage, les feedbacks utilisateur, et les éléments d'interface.

Fonctionnalités essentielles du jeu

Dans le jeu *SafeMobile Adventure*, le joueur doit se déplacer par des mouvements horizontal et vertical pour récupérer les 12 enveloppes, en évitant d'être touché par l'ennemi. Le joueur perd la capacité de déplacement lorsqu'il est touché par l'ennemi et doit répondre à des quizz pour retrouver cette capacité. Il perd également une vie chaque fois qu'il aura à répondre à un quizz. Les quizz apparaissent sous la forme des messages que le joueur doit évaluer si ce sont des messages d'hameçonnage ou des messages légitimes. Le joueur a une minute pour répondre à chaque quizz. Il n'aura droit qu'à un maximum de 5 quizz et 6 vies pour chaque niveau du jeu. Une fois toutes les enveloppes récupérées, le joueur aura gagné le niveau du jeu. Si le joueur perd toutes ses vies il aura perdu la partie de jeu. Les performances du joueur sur les quizz sont enregistrées dans une base de données. Les données enregistrées incluent le nom du joueur, la date, le score de base, les points bonus (en fonction du temps de résolution du quizz), l'issue de la partie de jeu (le niveau de jeu est-il gagné ou pas), le nombre de quizz répondus dans le niveau de jeu, et le score final (score de base auquel on ajoute les points bonus).

Calendrier de développement du jeu

Le développement du prototype du jeu sérieux s'est déroulé sur une période de 4 mois, structurée en plusieurs phases clés allant de la conception initiale à la finalisation du prototype. Voici le calendrier initial détaillé des différentes étapes du développement :

TABLEAU 4.1 : Calendrier de développement du jeu *SafeMobile Adventure*

ID	Title	Start Time	End Time
1	Développement des premiers concepts visuels	05/01/2024	05/31/2024
2	Développement des fonctionnalités de base	05/01/2024	05/31/2024
3	Création des premiers niveaux de jeu	06/01/2024	07/31/2024
4	Développement de l'interface utilisateur initiale	06/01/2024	06/30/2024
5	Réalisation des tests préliminaires	07/01/2024	07/31/2024
6	Recueil des retours des tests et apport des ajustements	07/01/2024	08/31/2024
7	Intégration des éléments sonores et des effets visuels supplémentaires	07/01/2024	07/31/2024
8	Réalisation des tests de qualité et correction des problèmes de performance	08/01/2024	08/31/2024
9	Finalisation des éléments visuels et sonores du jeu	08/01/2024	08/31/2024
10	Ajout des fonctionnalités de feedback	08/01/2024	08/31/2024
11	Tests approfondis sur toutes les fonctionnalités du jeu	08/01/2024	08/31/2024
12	Correction des bugs identifiés et réalisation des ajustements	07/01/2024	08/31/2024
13	Finalisation du développement du jeu	08/01/2024	08/31/2024
14	Finalisation de la documentation du jeu	08/01/2024	08/31/2024

Allocation des ressources nécessaires

Le développement du prototype du jeu a nécessité une allocation stratégique des ressources matérielles et logicielles pour garantir une progression efficace à travers chaque étape du projet. Les ressources requises ont été limitées, car la plupart des outils utilisés étaient basés en ligne ou peu exigeants en termes de puissance de calcul. Un ordinateur avec des capacités standard de traitement a suffi pour faire tourner Construct 3 et les outils de conception graphique. Des smartphones et tablettes fonctionnant sous Android ont été utilisés pour tester le prototype et vérifier sa compatibilité avec différentes résolutions d'écran.

L'utilisation de plateformes logicielles en ligne a permis un développement rapide et efficace. Le projet a été conçu de manière à minimiser les coûts, en s'appuyant principalement sur des outils gratuits ou peu coûteux, tout en garantissant la qualité du prototype. En somme, l'allocation des ressources a été optimisée pour répondre aux exigences du projet tout en restant économique et efficace.

4.3.2 PHASE 2 : DEVELOPPEMENT DES SCENARIOS ET MECANIQUES DE JEU

La deuxième phase s'est concentrée sur la création des scénarios de jeu. Les scénarios d'hameçonnage ont été développés pour représenter différents vecteurs de menaces comme les SMS ou les applications de messagerie, et différents types de menaces comme les fausses alertes de sécurité, les offres alléchantes, les faux avis de livraison ou les faux avis de facturation. Les mécaniques de feedback ont été intégrées pour offrir des réponses immédiates aux actions des utilisateurs, renforçant ainsi l'apprentissage.

Scénarios de messages d'hameçonnage

Dans cette section, nous présentons les scénarios de messages d'hameçonnage représentatifs pour certaines catégories.

FIGURE 4.1 : SMS d'une fausse alerte de sécurité

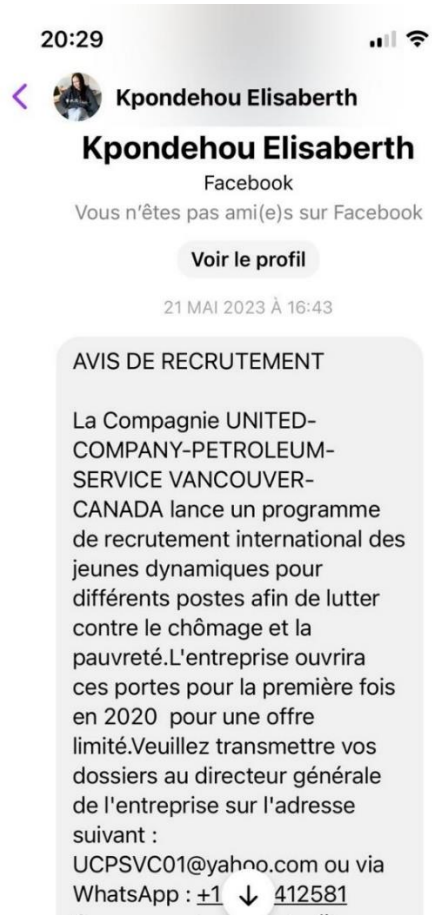

FIGURE 4.2 : Offre alléchante via une application de messagerie instantanée

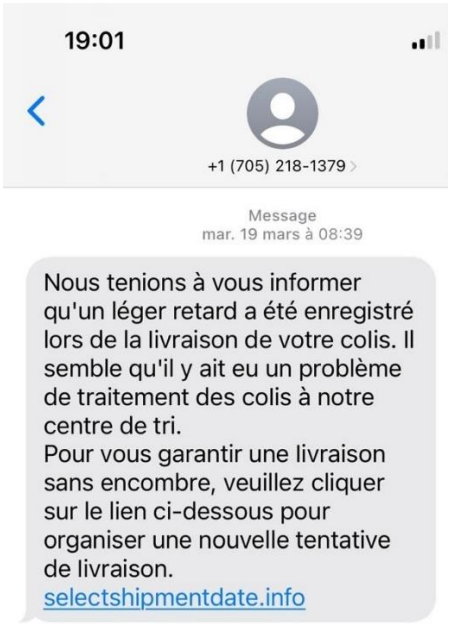

FIGURE 4.3 : SMS d'un faux avis de livraison

FIGURE 4.4 : SMS légitime

Feedbacks aux messages d'hameçonnage

Dans cette section, nous présentons les feedbacks représentatifs pour certaines catégories de messages d'hameçonnage. Il s'agit des feedbacks aux scénarios de messages présentés dans la section précédente.

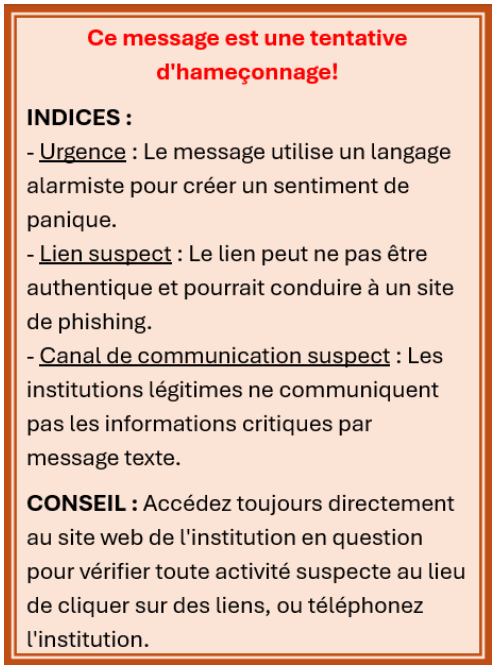

FIGURE 4.5 : Feedback pour une fausse alerte de sécurité

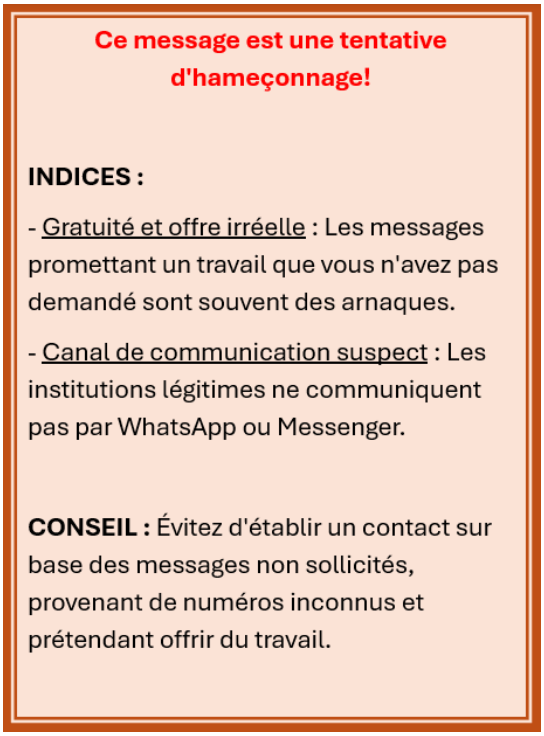

FIGURE 4.6 : Feedback pour une offre alléchante

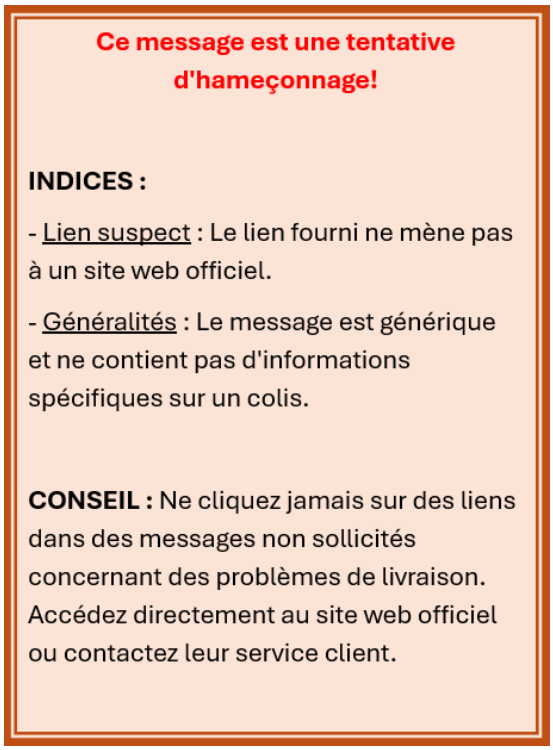

FIGURE 4.7 : Feedback pour un faux avis de livraison

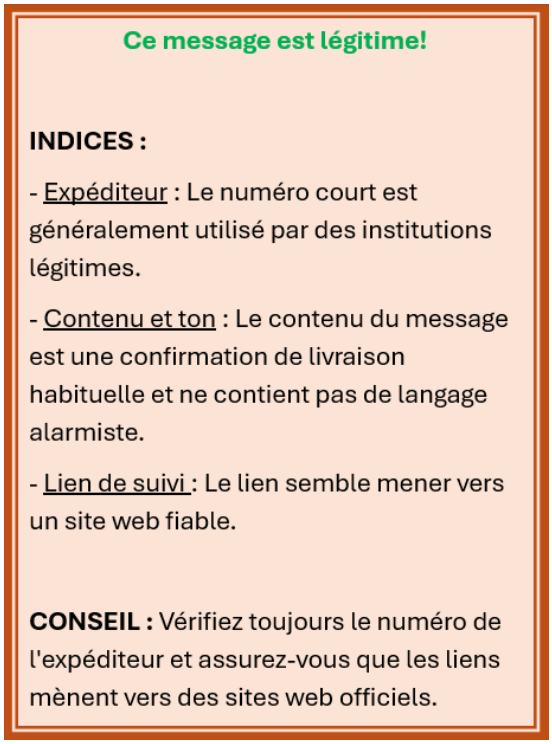

FIGURE 4.8 : Feedback pour un SMS légitime

4.3.3 PHASE 3 : CONCEPTION DE L'INTERFACE UTILISATEUR

Cette phase a été une étape cruciale dans le développement du prototype de *SafeMobile Adventure*. L'objectif principal de cette phase était de concevoir une interface utilisateur (UI) intuitive, attrayante et adaptée aux dispositifs mobiles, tout en intégrant des éléments visuels qui facilitent l'apprentissage et l'interaction avec le contenu du jeu.

Principes de conception

La conception de l'interface utilisateur a été guidée par plusieurs principes clés pour maximiser l'efficacité pédagogique et offrir une expérience utilisateur agréable :

Clarté et simplicité : L'interface a été conçue de manière à être minimaliste et claire, réduisant les distractions pour permettre aux utilisateurs de se concentrer sur les messages d'hameçonnage, les feedbacks et les défis du jeu. Chaque écran présente les informations essentielles, avec des boutons bien visibles et des options de navigation intuitives.

Accessibilité : Le design a été pensé pour être accessible à une large audience, indépendamment de leur âge ou niveau de familiarité avec les jeux vidéo. Des polices de caractères lisibles, des contrastes élevés, et des éléments de navigation explicites ont été utilisés pour s'assurer que le jeu soit utilisable par le plus grand nombre.

Consistance visuelle : Les éléments graphiques du jeu, comme les couleurs, les icônes, et les polices, ont été uniformisés tout au long du jeu pour offrir une expérience cohérente. Chaque écran suit la même logique de navigation, permettant aux joueurs de se familiariser rapidement avec les mécanismes du jeu.

Structure de l'interface

L'interface utilisateur de *SafeMobile Adventure* est structurée en plusieurs sections clés, qui permettent aux joueurs d'interagir de manière fluide avec le jeu :

Écran d'accueil : Cet écran accueille le joueur avec une introduction du jeu, des boutons « Jouer » et « Quitter ». Le design de cet écran vise à introduire rapidement le joueur dans l'univers du jeu sans surcharge d'informations.

FIGURE 4.9 : Ecran d'accueil du jeu *SafeMobile Adventure*

Écran des instructions : Cet écran contient les instructions du jeu avec le bouton « Commencer » pour débuter le jeu, et le bouton « Meilleurs scores » pour consulter les 10 meilleurs scores déjà réalisés.

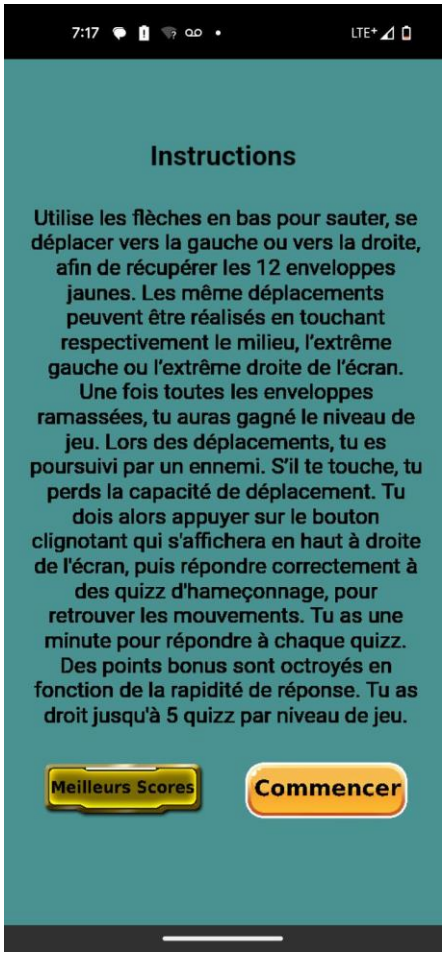

FIGURE 4.10 : Ecran des instructions du jeu *SafeMobile Adventure*

Écran des meilleurs scores : Cet écran présente les 10 meilleurs scores déjà réalisés dans le jeu, avec le bouton « Commencer » pour débuter le jeu.

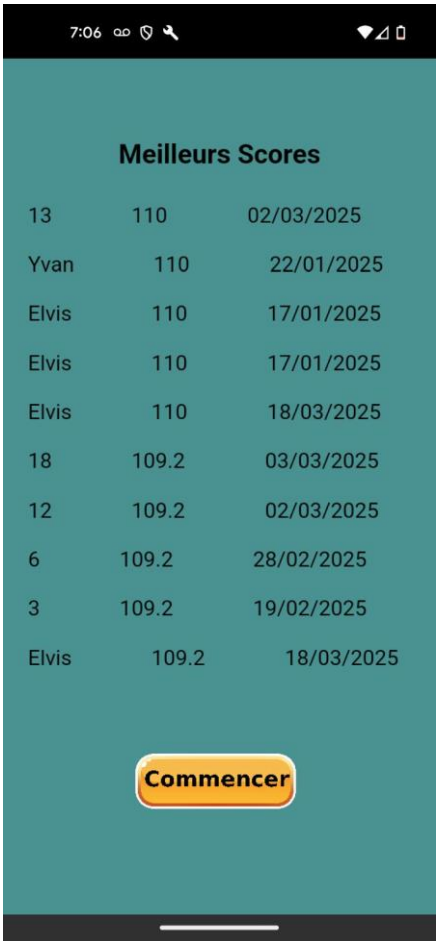

FIGURE 4.11 : Ecran des meilleurs scores du jeu *SafeMobile Adventure*

Interface de jeu principale : L'écran principal où le joueur interagit avec les éléments du jeu, les messages d'hameçonnage et les feedbacks, est conçu pour ressembler à celui d'une application de jeu standard.

FIGURE 4.12 : Ecran du premier niveau du jeu *SafeMobile Adventure*

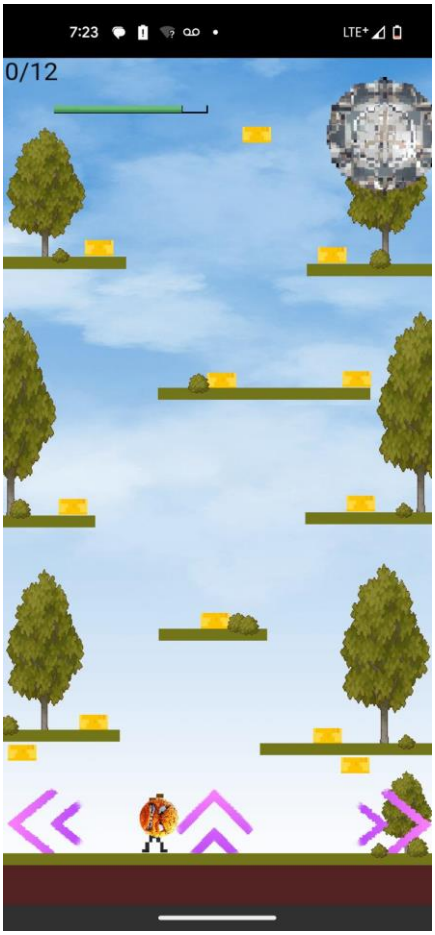

Figure 4.13 : Ecran du second niveau du jeu *SafeMobile Adventure*

Scénarios de messages et feedbacks : Les scénarios de messages et leurs feedbacks apparaissent sur l'interface de jeu principale. Après chaque décision du joueur, un message de retour d'information apparaît, expliquant pourquoi le message était (ou non) une tentative d'hameçonnage mobile. Ce message de retour utilise un design simple, avec des icônes et des textes explicatifs faciles à lire.

FIGURE 4.14 : Interface de jeu principale avec un scénario de message à évaluer

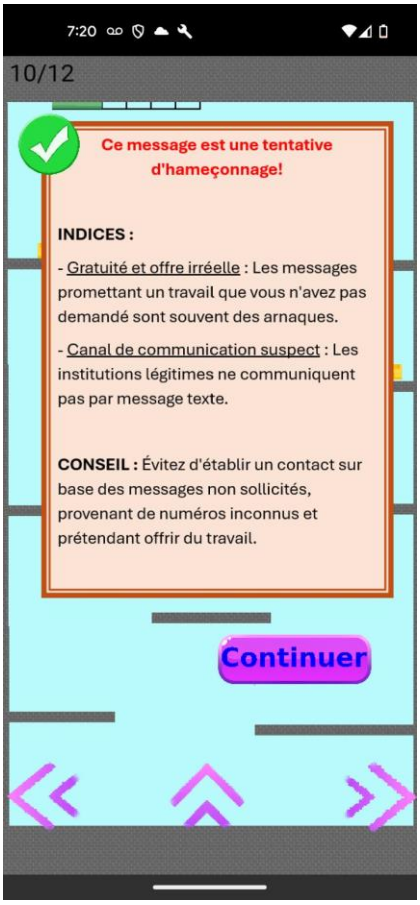

FIGURE 4.15 : Interface de jeu principale avec un feedback sur une bonne décision

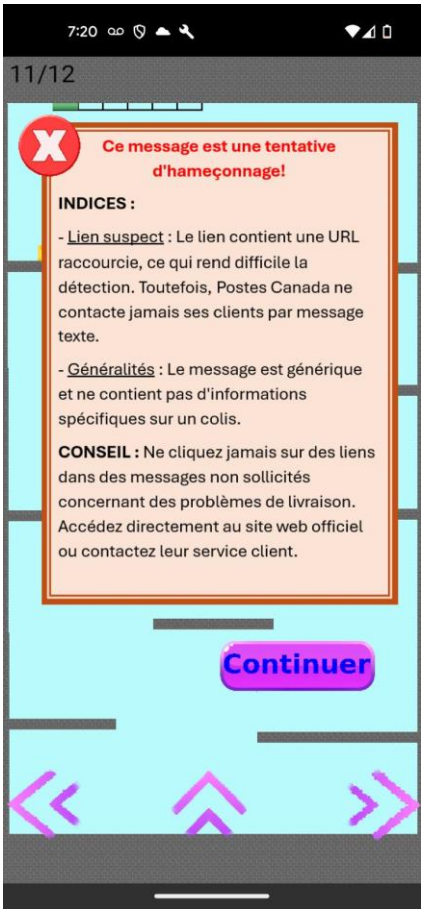

FIGURE 4.16 : Interface de jeu principale avec un feedback sur une mauvaise décision

Écrans de fin : Ces écrans présentent au joueur l'issue du niveau du jeu, avec des boutons qui permettent de reprendre le niveau après un échec, de continuer au niveau suivant après réussite, ou de quitter le jeu.

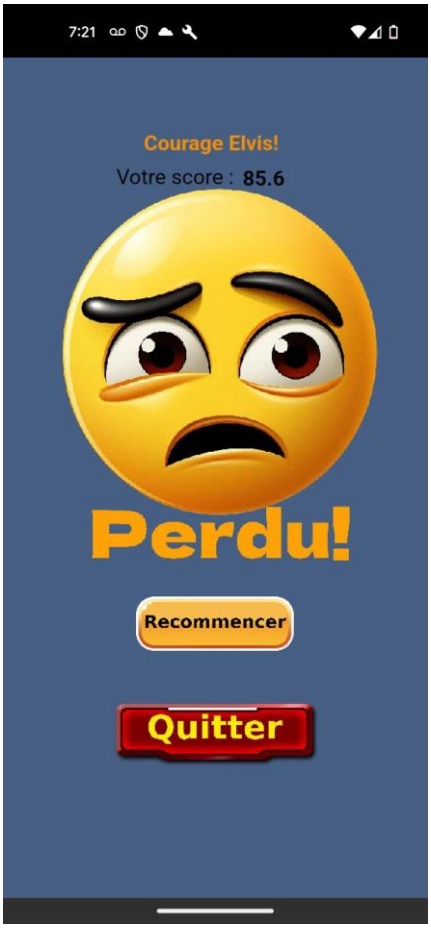

FIGURE 4.17 : Ecran d'échec à un niveau du jeu

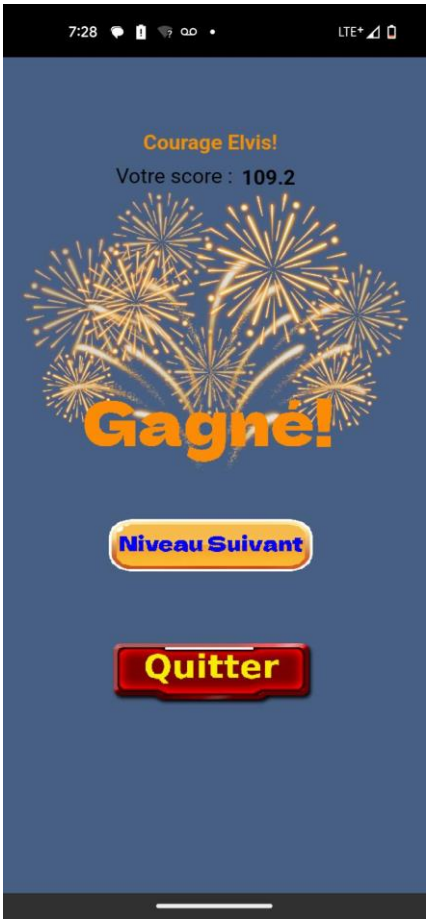

FIGURE 4.18 : Ecran de réussite au premier niveau du jeu

FIGURE 4.19 : Ecran de réussite au second niveau du jeu

Design des éléments visuels

Les éléments visuels de l'interface utilisateur ont été créés pour renforcer l'aspect éducatif du jeu tout en restant esthétiquement plaisants :

Couleurs : Une palette de couleurs douces et apaisantes a été utilisée pour les interfaces générales, afin de maintenir un environnement non stressant. Des couleurs plus vives sont appliquées aux boutons et alertes pour attirer l'attention sur les actions importantes.

Icônes : Des icônes familières, comme celles représentant une enveloppe, ont été intégrées pour rendre l'interface intuitive. Les icônes de feedback, telles que les coches vertes pour les bonnes réponses ou les croix rouges pour les erreurs, fournissent des indications visuelles claires sur la performance du joueur.

Typographie : Des polices de caractères simples ont été choisies pour garantir la lisibilité, même sur les petits écrans de smartphones. La taille des textes a été ajustée pour être suffisamment visible, plus particulièrement pour les feedbacks où l'attention est requise.

Tests d'ergonomie

L'interface utilisateur a fait l'objet de plusieurs tests d'ergonomie durant cette phase pour s'assurer qu'elle réponde aux besoins des joueurs en termes de facilité d'utilisation. Ces tests ont permis de recueillir des retours sur l'ergonomie de l'interface et d'apporter des ajustements, notamment en ce qui concerne la clarté des boutons et des feedbacks, la taille des éléments interactifs et la fluidité de la navigation entre les écrans.

4.3.4 PHASE 4 : TESTS ET DEBOGAGE

Une fois les fonctionnalités de base développées, le prototype a été soumis à une série de tests pour identifier les bugs et les problèmes d'ergonomie. Des tests unitaires ont été réalisés pour vérifier que chaque composant du jeu fonctionnait comme prévu. De plus, des tests utilisateurs ont été organisés avec un groupe restreint de volontaires pour recueillir des feedbacks sur l'expérience de jeu et l'efficacité des scénarios pédagogiques.

4.3.5 PHASE 5 : AMELIORATIONS ET AJUSTEMENTS

Les retours des tests utilisateurs ont conduit à plusieurs itérations du prototype. Des ajustements ont été faits pour améliorer la jouabilité, affiner les scénarios d'hameçonnage, et résoudre les problèmes techniques. Cette phase a également inclus l'optimisation de la performance du jeu sur différents appareils mobiles.

4.4 TESTS INITIAUX ET AMELIORATION DU PROTOTYPE

Le processus de développement d'un jeu sérieux ne se termine pas avec la création du prototype. Pour garantir son efficacité pédagogique et sa jouabilité, il est essentiel de passer par une phase rigoureuse de tests initiaux, suivie d'améliorations basées sur les résultats obtenus.

4.4.1 OBJECTIFS DES TESTS INITIAUX

Les tests initiaux avaient pour but de :

Évaluer l'expérience utilisateur : Vérifier que le jeu est intuitif, engageant, et qu'il maintient l'intérêt des utilisateurs tout au long des scénarios.

Mesurer l'efficacité pédagogique : S'assurer que les joueurs acquièrent des compétences en matière de détection d'hameçonnage mobile et qu'ils sont capables de les appliquer dans des contextes variés.

Identifier et corriger les bugs : Détecter les problèmes techniques, qu'il s'agisse de bugs mineurs ou de failles qui pourraient nuire à l'expérience de jeu.

Recevoir des retours qualitatifs : Recueillir les impressions des utilisateurs concernant le design, la pertinence des scénarios, et la clarté des instructions.

4.4.2 METHODOLOGIE DES TESTS

4.4.2.1 SELECTION DES TESTEURS

Un groupe diversifié de testeurs a été sélectionné pour participer aux tests initiaux. Ce groupe comprenait :

Des utilisateurs novices : Personnes avec peu ou pas de connaissances sur les techniques d'hameçonnage, afin de tester l'efficacité pédagogique du jeu.

Des experts en sécurité informatique : Pour évaluer la pertinence des scénarios d'hameçonnage et l'exactitude des informations fournies.

Des joueurs occasionnels : Utilisateurs ayant une certaine expérience des jeux mobiles pour juger de la jouabilité et de l'interface.

4.4.2.2 PROTOCOLES DE TEST

Chaque testeur a été invité à jouer plusieurs niveaux du prototype, en prenant en compte les éléments suivants :

Facilité de navigation : Mesurer si les utilisateurs trouvaient les menus et les interactions intuitives.

Réactivité et performance : Observer le temps de réponse du jeu, en particulier sur différents modèles de smartphones.

Compréhension et apprentissage : Poser des questions aux testeurs après chaque session pour évaluer ce qu'ils ont retenu des scénarios et des feedbacks.

Satisfaction générale : Recueillir des retours sur l'expérience globale, incluant le plaisir de jouer, l'intérêt suscité, et les suggestions d'amélioration.

4.4.3 RESULTATS DES TESTS

Les résultats des tests ont fourni une vue d'ensemble précieuse sur la performance du prototype, avec des points forts et des domaines nécessitant des ajustements :

4.4.3.1 POINTS FORTS

Interface utilisateur intuitive : La majorité des testeurs ont trouvé l'interface claire et facile à utiliser, facilitant ainsi la prise en main rapide du jeu.

Scénarios réalistes : Les utilisateurs ont souligné la pertinence des scénarios d'hameçonnage, qui reflétaient bien les types de menaces qu'ils pouvaient rencontrer dans la vie réelle.

Efficacité pédagogique : Les retours ont montré que le jeu a réussi à sensibiliser les utilisateurs, augmentant leur vigilance face aux messages suspects.

4.4.3.2 PROBLEMES IDENTIFIES

Difficulté inégale : Certains testeurs ont trouvé que la difficulté des niveaux n'était pas toujours bien équilibrée, avec des sauts brusques entre des scénarios trop simples et d'autres trop complexes.

Bugs mineurs : Quelques bugs techniques ont été identifiés, comme des scénarios de messages ou des feedbacks qui mettaient plus de temps à s'afficher.

Feedbacks peu détaillés : Certains utilisateurs ont mentionné que certains feedbacks sur leurs choix dans le jeu manquaient de détails, ce qui limitait leur capacité à comprendre pleinement leurs erreurs.

4.4.4 AMELIORATIONS DU PROTOTYPE

Sur la base des retours obtenus, plusieurs améliorations ont été apportées au prototype pour résoudre les problèmes identifiés et optimiser l'expérience utilisateur. L'optimisation de la performance du jeu a été effectuée pour améliorer la réactivité sur différents appareils mobiles, en particulier ceux de milieu de gamme ou plus anciens. Cela a inclus notamment la compression des ressources graphiques et la simplification de certains effets visuels pour réduire la charge sur les processeurs.

4.5 DEFIS RENCONTRES ET SOLUTIONS

Le développement du prototype a rencontré plusieurs défis, notamment :

Compatibilité entre appareils : Garantir que le jeu fonctionne de manière homogène sur diverses résolutions d'écrans a nécessité des ajustements spécifiques et des tests supplémentaires.

Gameplay : Il a été crucial de transformer le gameplay pour qu'il soit plus motivant et engageant.

Gestion des ressources : Le développement du prototype avec des ressources limitées a demandé une gestion rigoureuse du temps et des priorités.

Pour surmonter ces défis, des ajustements continus ont été faits, des outils de monitoring de performance ont été utilisés, et des tests fréquents ont permis de garantir que le prototype répondait aux attentes.

4.6 RESULTATS ET VALIDATION DU PROTOTYPE

Le prototype final a atteint les objectifs initialement fixés. Les tests utilisateurs ont montré que le jeu était engageant et efficace pour sensibiliser les utilisateurs aux dangers de l'hameçonnage mobile. Les retours ont également révélé que les utilisateurs étaient capables de transférer les connaissances acquises dans le jeu à des situations réelles, validant ainsi l'approche pédagogique du prototype.

4.7 CONCLUSION

Le développement du prototype a été une étape essentielle pour transformer les concepts théoriques en un outil pédagogique concret. Grâce à l'utilisation d'outils de développement modernes et à une approche méthodologique itérative, le prototype a non seulement démontré sa faisabilité technique, mais aussi son potentiel éducatif. La phase de tests initiaux et les améliorations qui en ont découlé ont été essentielles pour affiner le prototype du jeu sérieux. Ces ajustements ont permis non seulement d’améliorer la jouabilité et la performance du jeu, mais aussi d’assurer que les objectifs pédagogiques soient atteints de manière plus efficace. Le prototype ainsi optimisé est désormais prêt pour des tests plus larges et pour l’évaluation finale, qui détermineront son aptitude à être déployé dans des contextes réels de sensibilisation à l’hameçonnage mobile.

CHAPITRE V

ÉVALUATION DE L'EFFICACITÉ DU JEU

5.1 INTRODUCTION

L'objectif de cette phase est d'évaluer l'efficacité du jeu sérieux *SafeMobile Adventure* en mesurant son impact sur la sensibilisation des utilisateurs à l'hameçonnage mobile. Cette évaluation repose sur une expérimentation menée auprès d'un échantillon de participants, à travers des tests finaux comprenant une session de jeu, des questionnaires préliminaires et post-intervention. L'analyse des résultats recueillis permet d'examiner les progrès des joueurs en termes de reconnaissance des tentatives d'hameçonnage et de leur changement de comportement face à ces menaces.

5.2 METHODOLOGIE D'EVALUATION

5.2.1 PARTICIPANTS

Un total de 20 participants a été recruté pour cette étude. Les participants ont été sélectionnés parmi des étudiants ayant des niveaux de connaissances variés en matière de sécurité informatique. Les graphiques qui suivent montrent respectivement la répartition des participants selon le genre et l'âge

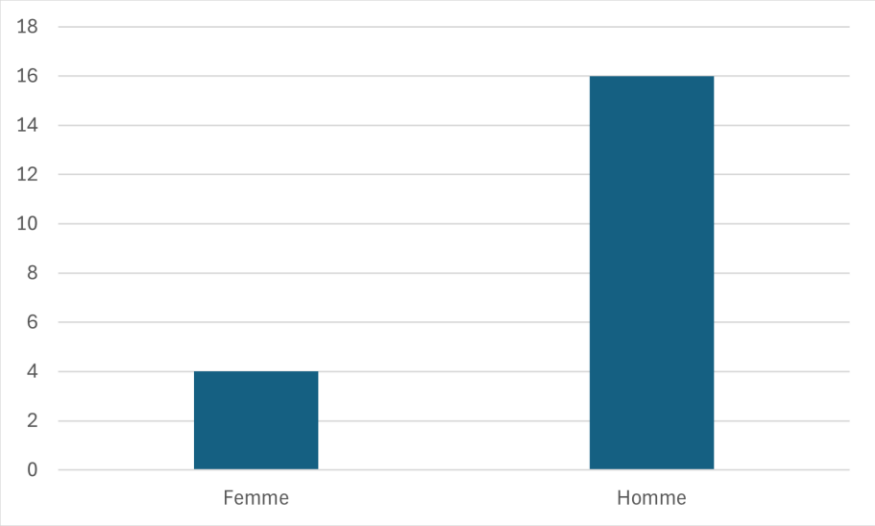

FIGURE 5.1 : Répartition des participants selon le genre

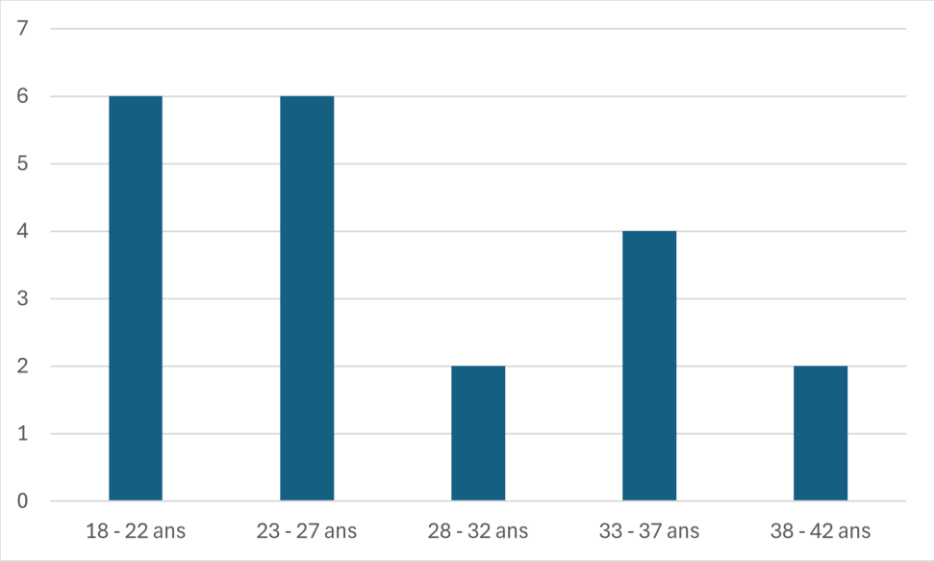

FIGURE 5.2 : Répartition des participants selon l'âge

5.2.2 PROTOCOLE EXPERIMENTAL

L'évaluation s'est déroulée en trois étapes :

1. **Questionnaire préliminaire** : Mesure des connaissances initiales des participants sur l'hameçonnage mobile avant l'utilisation du jeu.
2. **Session de jeu** : Les participants ont joué à *SafeMobile Adventure* pendant environ 30 minutes.

3. **Questionnaire post-intervention** : Évaluation des connaissances et du changement de comportement après l'expérience de jeu.

Les réponses ont été analysées quantitativement et qualitativement afin d'évaluer l'impact du jeu sur la compréhension et la prévention des attaques d'hameçonnage. Il est à noter qu'aucune information permettant d'identifier un participant n'a été recueillie. Un code numérique a été utilisé pour lier les questionnaires utilisés par chaque participant aux performances dans la session de jeu.

5.3 ANALYSE DES RESULTATS

5.3.1 RESULTATS DU QUESTIONNAIRE PRELIMINAIRE

Avant l'expérience de jeu, les participants ont répondu à un questionnaire mesurant leurs connaissances et comportements face à l'hameçonnage mobile. Voici quelques résultats synthétiques des réponses obtenues :

- **Fréquence d'utilisation du smartphone :** 50 % des participants ont déclaré utiliser leurs smartphones *plus de 6 heures par jour*, 45 % *entre 4 et 6 heures par jour*, et 5 % *entre 1 et 3 heures par jour*.
- **Activités principales sur le smartphone :** plus de 95 % des participants ont déclaré utiliser leurs smartphones pour les *appels*, les *messages*, la *navigation sur Internet*, les *courriels* et les *transactions bancaires* ; 40 % d'entre eux ont affirmé en utiliser en plus pour les *jeux*.
- **Connaissances sur l'hameçonnage mobile :** 60 % des participants ont déclaré n'avoir *jamais entendu parler du terme « hameçonnage mobile »*, 40 % des participants ont déclaré *avoir été victime ou connaitre quelqu'un qui a été victime d'une attaque par hameçonnage mobile*, 80 % des participants ont déclaré *savoir identifier un message d'hameçonnage mobile*.

- **Fréquence de réception des messages d'hameçonnage mobile :** 20 % des participants ont déclaré recevoir *souvent* des messages d'hameçonnage mobile, 40 % ont déclaré en recevoir *parfois*, 30 % *rarement*, et 10 % *jamais*.
- **Action à la réception d'un message d'hameçonnage mobile :** 95 % des participants ont déclaré *ignorer, signaler et/ou supprimer* les messages qu'ils jugent être des messages d'hameçonnage mobile, tandis que 5 % ont déclaré *cliquer sur le lien* du message pour vérifier.
- **Niveau de risque d'être victime de l'hameçonnage mobile :** 35 % des participants ont estimé que le risque d'être victime de l'hameçonnage mobile est *élevé*, 35 % ont estimé que le risque est *modéré*, 25 % ont estimé qu'il est *faible*, alors que 5 % ont estimé que ce risque est *très élevé*.
- **Niveau de connaissance actuel de l'hameçonnage mobile :** 75 % des participants ont estimé avoir un niveau de connaissance *modéré* sur les attaques par hameçonnage mobile, 20 % ont estimé avoir un niveau *faible*, alors que 5 % ont estimé avoir un niveau *élevé*.

Ces résultats montrent un certain écart chez les participants, en ce qui concerne les connaissances et les comportements adoptés face aux attaques par hameçonnage mobile, ce qui justifie la nécessité d'un outil éducatif tel que *SafeMobile Adventure*.

5.3.2 RESULTATS DE LA SESSION DE JEU

Lors de la session de jeu, 19 participants ont joué au moins 5 parties de jeu à l'une ou les 2 niveaux du jeu. Un participant a joué seulement 3 parties de jeu. Leurs performances sur la reconnaissance des messages d'hameçonnage mobile ont été recueillies dans une base de données. En raison du fait que les scénarios de messages sont affichés de manière aléatoire dans le jeu, nous avons jugé bon de considérer pour notre analyse, le plus bas score pour les premières parties de jeu, et le score le plus élevé pour les dernières parties de jeu. Les résultats synthétiques sont soulignés dans le tableau qui suit :

TABLEAU 5.1 : Résultats de la session de jeu

Participant	Premières parties de jeu	Dernières parties de jeu	Progression
1	60 %	80 %	20 %
2	40 %	66,6 %	26,6 %
3	40 %	100 %	60 %
4	40 %	100 %	60 %
5	20 %	40 %	20 %
6	60 %	100 %	40 %
7	60 %	100 %	40 %
8	60 %	100 %	40 %
9	80 %	100 %	20 %
10	80 %	80 %	0 %
11	75 %	100 %	25 %
12	60 %	100 %	40 %
13	40 %	100 %	60 %
14	40 %	80 %	40 %
15	60 %	80 %	20 %
16	60 %	80 %	20 %
17	80 %	100 %	20 %
18	40 %	100 %	60 %
19	20 %	80 %	60 %
20	40 %	100 %	60 %
Moyenne			
	52,75 %	89,33 %	36,58 %

Les résultats de la session de jeu démontrent une amélioration significative de 36,58 % pour ce qui est de la reconnaissance des tentatives d'hameçonnage mobile.

5.3.3 RESULTATS DU QUESTIONNAIRE POST-INTERVENTION

Après avoir joué, les mêmes participants ont complété un second questionnaire, afin d'évaluer l'évolution de leurs connaissances et comportements, ainsi que leur expérience de jeu en général. Ci-après les résultats synthétiques des réponses obtenues :

- **Expérience avec le jeu :** 55 % des participants ont déclaré être *satisfait* de leur expérience avec le jeu, alors que 45 % ont déclaré être même *très satisfait*.
- **Facilité à comprendre et à jouer :** 45 % des participants ont déclaré que le jeu était *facile* à comprendre et à jouer, alors que 20 % ont déclaré qu'il était même *très facile*, 15 % des participants étaient *neutres*.
- **Clarté des instructions du jeu :** 65 % des participants ont déclaré que les instructions étaient *claires* pour comprendre les objectifs et les tâches à accomplir, alors que 15 % ont déclaré qu'elles étaient même *très claires*.
- **Durée des niveaux du jeu :** 90 % des participants ont déclaré que la durée des niveaux de jeu était *appropriée*, alors que 10 % ont déclaré qu'elle était *courte*.
- **Capacité à identifier l'hameçonnage mobile :** 50 % des participants ont déclaré que le jeu a *beaucoup* amélioré leur capacité à identifier un message d'hameçonnage mobile, tandis que 40 % ont déclaré que le jeu a même *énormément* amélioré cette capacité.
- **Situation réaliste d'hameçonnage mobile :** 45 % des participants ont déclaré que le jeu présentait des situations *réalistes* d'hameçonnage mobile, tandis que 50 % ont déclaré que ces situations étaient même *très réalistes*.
- **Modification des comportements :** après avoir joué au jeu, 55 % des participants ont déclaré que le jeu les aidera *beaucoup* à modifier leur comportement face à un message suspect, tandis que 35 % ont déclaré que le jeu les aidera même *énormément* à modifier leur comportement.
- **Comportement face à un message d'hameçonnage mobile :** après avoir joué au jeu, 90 % des participants ont déclaré qu'ils *supprimeraient et/ou signaleraient* un message qui semble être de l'hameçonnage mobile, et 10 % ont déclaré qu'ils *ignoreraient* le message.

- **Contribution du jeu :** 45 % des participants ont déclaré que le jeu pourrait ***beaucoup*** aider d'autres utilisateurs de smartphones à mieux se protéger contre l'hameçonnage mobile, tandis que 45 % ont déclaré qu'il pourrait aider même ***énormément***.
- **Qualité graphique et visuelle :** 40 % des participants ont déclaré que la qualité graphique et visuelle du jeu était ***bonne***, alors que 55 % ont déclaré qu'elle était ***moyenne***.
- **Recommandation du jeu :** enfin, 100 % des participants ont déclaré qu'ils ***recommanderaient le jeu*** à d'autres personnes dans le but de les sensibiliser à l'hameçonnage mobile.

> Les résultats du questionnaire post-intervention indiquent que *SafeMobile Adventure* a permis une amélioration significative des connaissances et des comportements en matière de cybersécurité.

5.3.4 RETOURS QUALITATIFS DES PARTICIPANTS

En plus des résultats quantitatifs, des commentaires ont été recueillis auprès des participants :

❖ **Points positifs :**

- « Le jeu a amélioré ma compréhension de l'hameçonnage et ma capacité à mieux me protéger. »
- « L'expérience de jeu était très enrichissante et instructive, j'ai appris plein de nouvelles choses. »
- « Jeu efficace pour sensibiliser les gens à détecter les messages pour but de fraude. »
- « Le jeu est très important pour apprendre à détecter l'hameçonnage mobile. »
- « Je me suis amusée tout en apprenant. »

❖ **Suggestions d'amélioration :**

- Ajout des illustrations dans les instructions du jeu pour qu'elles soient beaucoup plus claires.

- Amélioration de l’interface utilisateur (montrer l’évolution du score pendant une session de jeu, améliorer le design en ajoutant plus d’éléments graphiques). Cette suggestion pourrait être un peu difficile à mettre en œuvre à cause de la taille d’un écran de smartphone.
- Amélioration de la facilité de déplacement du personnage du jeu. Nous avons constaté que cette suggestion a été émise par quelques participants qui avaient démontré une certaine incapacité à manipuler aisément leurs smartphones lors des sessions de jeu, du fait qu’ils n’étaient pas habitués à jouer sur leurs téléphones.

5.4 DISCUSSION

Les résultats de la session de jeu et du questionnaire post-intervention montrent une nette amélioration des connaissances et des comportements des participants après leur exposition au jeu sérieux. En comparant la performance des joueurs dans les premières et les dernières parties de jeu, nous avons observé une amélioration significative dans leur habileté d’identification de smishing et d’autres tentatives d’hameçonnage mobile. La progression était positive pour 19 participants, et nulle pour seulement un participant. Pour le participant dont la progression était nulle, nous avons constaté dans le questionnaire préliminaire, qu'il avait indiqué savoir identifier un message d'hameçonnage, et avait également affirmé supprimer immédiatement un message qu’il juge suspect. Il avait aussi déclaré utiliser des outils de sécurité sur son smartphone.

La satisfaction générale des utilisateurs a été élevée, avec la quasi-totalité de participants exprimant leur intention de recommander le jeu à d'autres personnes pour les sensibiliser à l'hameçonnage mobile. La jouabilité, les scénarios de messages d’hameçonnage mobile, ainsi que la qualité des feedbacks, ont été particulièrement appréciées. L’augmentation du taux de reconnaissance des tentatives d’hameçonnage et l’adoption des bonnes pratiques indique que *SafeMobile Adventure* est un outil efficace pour la sensibilisation aux cybermenaces.

5.5 LIMITATIONS DE L'ETUDE

L'échantillon de participants étant relativement restreint et non représentatif de l'ensemble des utilisateurs de téléphones mobiles, la généralisation des résultats à une population plus large demeure limitée. De plus, les tests ont été réalisés sur un seul type d'appareil (Google Pixel 8), ce qui restreint l'évaluation à une configuration matérielle spécifique. Les recherches futures devraient envisager un groupe de participants plus diversifié, et d'autres configurations matérielles.

Une autre limitation réside dans l'ordre de présentation des scénarios de messages d'hameçonnage. Dans le jeu, les messages sont affichés de façon aléatoire, ce qui peut entraîner une variabilité dans la difficulté perçue entre les premières et les dernières parties de jeu. Cette variation pourrait influencer l'évaluation de la progression de l'utilisateur durant la session de jeu, notamment si les scénarios les plus faciles ou les plus difficiles sont regroupés au début ou à la fin de la séance. Malgré ce défi, nous pouvons toujours nous fier aux résultats du questionnaire post-intervention.

Le processus d'évaluation, qui comprend un questionnaire préliminaire, une séance de jeu et un questionnaire post-intervention, repose en partie sur des données autodéclarées, notamment via le questionnaire post-intervention. Les participants peuvent avoir surestimé ou sous-estimé leurs résultats d'apprentissage en raison d'une mauvaise appréciation de leur progression réelle. Cependant, étant donné que la performance de la session de jeu a été enregistrée, cela devrait réduire l'impact de ce défi.

Il est possible que certains éléments de l'interface aient influencé involontairement les performances des participants. Par exemple, l'interface graphique a été jugée moins satisfaisante que les autres aspects du jeu par certains utilisateurs, ce qui pourrait avoir affecté leur expérience d'apprentissage. Une interface mal conçue peut entraîner une diminution de la motivation, limitant ainsi le potentiel éducatif du jeu. Les versions futures du jeu devraient répondre aux problèmes de convivialité pour garantir une expérience utilisateur intuitive.

Certaines limites de cette étude sont liées à des facteurs potentiellement non contrôlés sur les participants, tels que la connaissance préalable sur l'hameçonnage, les différences de capacités cognitives, ou le niveau d'implication pendant le jeu, qui pourraient influencer les conclusions tirées. Les recherches futures devraient envisager des modèles expérimentaux plus contrôlés.

CONCLUSION

La présente recherche a exploré le développement et l'évaluation d'un jeu sérieux visant à sensibiliser les utilisateurs à l'hameçonnage mobile. Face à l'essor des cyberattaques ciblant les appareils mobiles et à la vulnérabilité croissante des utilisateurs, cette étude a proposé une solution pédagogique combinant ludification et formation en cybersécurité.

L'analyse de la littérature a permis d'établir le contexte théorique et technique du projet en mettant en évidence les mécanismes d'hameçonnage mobile, les approches existantes de sensibilisation et le potentiel des jeux sérieux comme outil d'apprentissage. La phase de développement du jeu a intégré des principes pédagogiques et ergonomiques favorisant l'acquisition de compétences en reconnaissance des attaques d'hameçonnage. L'utilisation d'un moteur de jeu accessible et de ressources graphiques et sonores adaptées a permis le développement d'un prototype fonctionnel. L'évaluation du jeu, basée sur des tests finaux impliquant des utilisateurs, a mis en évidence une amélioration significative de la capacité des participants à identifier les tentatives d'hameçonnage. Les résultats obtenus ont confirmé la pertinence du jeu comme outil de sensibilisation et ont également mis en exergue des axes d'amélioration pour une adoption plus large.

En perspective, le projet pourrait être enrichi par l'intégration d'une intelligence artificielle adaptant dynamiquement les scénarios d'apprentissage à l'utilisateur. Par ailleurs, une étude à plus grande échelle pourrait renforcer la validation de l'efficacité de cette approche.

En conclusion, ce travail ouvre la voie à une nouvelle manière de sensibiliser le public aux risques de l'hameçonnage mobile et met en avant le potentiel des jeux sérieux comme outil pédagogique dans le domaine de la cybersécurité.

BIBLIOGRAPHIE

Abrahamsson, P., Salo, O., Ronkainen, J., & Warsta, J. (2017). Agile software development methods: Review and analysis. *arXiv preprint arXiv:1709.08439*.

André, B. (2023, 18 septembre). Comment repérer l'hameçonnage par SMS. *Le Journal de Montréal*. https://www.journaldemontreal.com/2023/09/18/comment-identifier-lhameconnage-par-sms

Anna, F. (2022, 15 avril). *Spam Text Messages (SMS) — How to Stop or Block Spam Texts*. Avast Academy. https://www.avast.com/fr-fr/c-how-to-stop-spam-text-messages

Badreau, S. p. (2021). *Gestion de projet agile*. Editions ENI.

Butt, U. J. (2023). *Developing a Usable Security Approach for User Awareness Against Ransomware* [PhD Thesis, Brunel University]. https://bura.brunel.ac.uk/handle/2438/26661

Cai, Y., Zhang, S., Xia, H., Fan, Y., & Zhang, H. (2020). A Privacy-Preserving Scheme for Interactive Messaging Over Online Social Networks. *IEEE Internet of Things Journal*, *7*(8). https://doi.org/10.1109/JIOT.2020.2986341

Centre antifraude du Canada. (2024). *Hameçonnage*. https://antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-hameconnage-fra.htm

Centre canadien pour la cybersécurité. (2022). *Ne mordez pas à l'hameçon : reconnaître et prévenir les attaques par hameçonnage*. https://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2020/20-16/publications.gc.ca/collections/collection_2020/cstc-csec/D97-1-00-101-2020-fra.pdf

Centre de la sécurité des télécommunications. (2021). *L'histoire de l'hameçonnage*. https://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2021/21-42/publications.gc.ca/collections/collection_2021/cstc-csec/D96-69-2021-fra.pdf

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, *27*(6), 581-612. https://doi.org/10.3233/JCS-181253

Gamagedara Arachchilage, N. A. (2012). *Security Awareness of Computer Users: A Game Based Learning Approach* [PhD Thesis, Brunel University]. https://bura.brunel.ac.uk/handle/2438/7620

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, *73*, 519-544. https://doi.org/10.1016/j.cose.2017.12.006

Hocine, N., Gouaich, A., Lylia, A., & Di Loreto, I. (2011). Etat de l'art des techniques d'adaptation dans les jeux ludiques et sérieux. *Revue d'Intelligence Artificielle*, *25*, 253-280. https://doi.org/10.3166/ria.25.253-280

Ivanov, M. A., Kliuchnikova, B. V., Chugunkov, I. V., & Plaksina, A. M. (2021, 26-29 january). Phishing Attacks and Protection Against Them. 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia.

Jain, A. K., Debnath, N., & Jain, A. K. (2022). APuML: An Efficient Approach to Detect Mobile Phishing Webpages using Machine Learning. *Wireless Personal Communications : An International Journal*, *125*(4), 3227-3248. https://doi.org/10.1007/s11277-022-09707-w

Kaspersky. (2024). *What is Smishing and How to Defend Against it*. https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Laricchia, F. (2024, 15 october). *Smartphones - statistics & facts*. Statista. https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

Matthew, K. (2024, 10 june). *What is smishing (SMS phishing)?.* IBM. https://www.ibm.com/topics/smishing

Meinel, C., Leifer, L., & Plattner, H. (2011). *Design Thinking: Understand – Improve – Apply*. Springer. https://doi.org/10.1007/978-3-642-13757-0

Microsoft. (2024). *Protégez-vous contre l'hameçonnage*. https://support.microsoft.com/fr-fr/windows/prot%C3%A9gez-vous-contre-l-hame%C3%A7onnage-0c7ea947-ba98-3bd9-7184-430e1f860a44

Misra, G., Arachchilage, N. A. G., & Berkovsky, S. (2017, 1 october). Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. International Symposium on Human Aspects of Information Security and Assurance, Adelaide, Australia.

Mostafa, M., & Faragallah, O. (2019). Development of Serious Games for Teaching Information Security Courses. *IEEE Access*, *7*, 169293-169305. https://doi.org/10.1109/ACCESS.2019.2955639

Muhly, F., Leo, P., & Caneppele, S. (2022). A Serious Game for Social Engineering Awareness Creation. *Journal of Cybersecurity Education, Research and Practice*, *2022*(1), Article 5. https://doi.org/10.62915/2472-2707.1101

Newbould, M., & Furnell, S. (2009, 1-3 december). Playing Safe: A Prototype Game For Raising Awareness of Social Engineering. Australian Information Security Management Conference, Perth, Western Australia.

Olanrewaju, A.-S. T., & Zakaria, N. H. (2015, 11-13 august). Social engineering awareness game (SEAG): an empirical evaluation of using game towards improving information security awareness. ICOCI 2015 - 5th International Conference on Computing and Informatics, Istanbul, Turkey.

Onashoga, A. S., Ojo, O. E., & Soyombo, O. O. (2019). Securix: a 3D game-based learning approach for phishing attack awareness. *Journal of Cyber Security Technology*, *3*(2), 108-124. https://doi.org/10.1080/23742917.2019.1624011

OneSpan. (2024). *Détection de la fraude mobile*. https://www.onespan.com/fr/topics/detection-de-la-fraude-mobile

Pensez cybersécurité. (2021). *Hameçonnage: Ne vous laissez pas prendre*. https://www.pensezcybersecurite.gc.ca/fr/hameconnage

Proofpoint. (2024). *What Is Smishing?* https://www.proofpoint.com/us/threat-reference/smishing

Purkait, S. (2012). Phishing counter measures and their effectiveness - literature review. *Information Management & Computer Security*, *20*(5), 382-420. https://doi.org/10.1108/09685221211286548

Schafer, T. (2018). Developing Threats in Mobile Phishing. *Credit Union Times*, *29*(16), 1-2. https://search-ebscohost-com.sbiproxy.uqac.ca/login.aspx?direct=true&db=bth&AN=142359194&lang=fr&site=ehost-live

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile Phishing Attacks and Mitigation Techniques. *Journal of Information Security*, *06*, 206-212. https://doi.org/10.4236/jis.2015.63021

Trudel, P., Abran, F., Dupuis, G. (2007). *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions* (Version du 26/04/07 ed.). Ministère des services gouvernementaux du Québec. http://collections.banq.qc.ca/ark:/52327/1565475

Verizon. (2020). *2020 Mobile Security Index Report: User threats* (2020 MSI). https://www.verizon.com/business/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Verizon. (2023). *2023 Data Breach Investigations Report* (2023 DBIR). https://www.verizon.com/business/resources/T636/reports/2023-data-breach-investigations-report-dbir.pdf

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296. https://doi.org/10.1016/j.chb.2019.07.034

Weanquoi, P., Johnson, J., & Zhang, J. (2018). Using a Game to Improve Phishing Awareness. *Journal of Cybersecurity Education, Research and Practice*, *2018*, Article 2. https://doi.org/10.62915/2472-2707.1040

CERTIFICATION ETHIQUE

Ce mémoire a fait l'objet d'une certification éthique auprès du CER-UQAC. Le numéro du certificat est **2025-1970**.