RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
https://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Yannick Etienne Sèdjro **ASSOSSOU**

Mise en place de campagnes de sensibilisation à la sécurité numérique à l'endroit des utilisateurs du MCVT

Sous la supervision :
Laurel **LISHOU**

Membres du jury :

SANYA Max Fréjus	Docteur	Président
KASSA Célia	Ingénieure	Examinatrice
LISHOU Laurel	Ingénieur	Rapporteur

Année Académique : **2022-2023**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire ix

Introduction 2

1 Revue de Littérature 4

2 Choix, installation du LMS et mise en place des campagnes de sensibilisation 7

3 Résultats 16

Conclusion 23

Annexe 24

Bibliographie 28

Webographie 29

Table des matières 30

Dédicace

A
Mon père Gislain ASSOSSOU
Ma mère Gilthère AISSE
Mon frère et ma soeur
Toute ma famille
Mes amis et mes proches

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui nous voudrions témoigner toute notre reconnaissance. Nous remercions sincèrement :

- le Professeur Eugène C. EZIN, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI) pour ses conseils et la formation qu'il nous a donné ;
- M. Laurel LISHOU, le superviseur de ce travail pour son accord à nous suivre, sa bienveillance, ses conseils et sa disponibilité ;
- M. Abdou Aziz SOBABE, M. Sabin SONON et M. Philippe KOSSOLOU, pour avoir respectivement accepté notre stage et nous avoir guidé dans l'exécution de ce travail ;
- tout le corps professoral de l'IFRI qui œuvre pour fournir les outils nécessaires à la réussite de nos études universitaires ;
- la famille et les amis qui nous ont soutenu et continuellement motivé à travailler et à terminer notre travail de recherche.

Que toutes les personnes qui ont contribué de près ou de loin au bon déroulement de ce travail voient en ces mots l'expression de profonde gratitude.

Résumé

Dans ce monde toujours plus connecté, de nombreux défis numériques se dressent devant nous. Au nombre de ceux-ci, assurer la sécurité des données présentes dans nos systèmes d'informations en toute circonstance se démarque comme l'un des plus sensibles, importants. Dans le but de faire face convenablement à ce défi de taille, de nombreuses mesures sont mises en place telles que les contrôles d'accès, le chiffrement des données, le Plan de Reprise d'Activité (PRA), le Plan de Continuité d'Activité (PCA), la sensibilisation, etc. Parmi ces mesures, une des plus cruciales est la sensibilisation à la sécurité numérique.
Notre travail a pour objectif de faire de la sensibilisation à la sécurité numérique à l'endroit des utilisateurs du Ministère du Cadre de Vie et des Transports afin qu'ils soient des utilisateurs avertis, et par conséquent une ligne de défense solide participant à la sécurité des données de leur structure. Pour ce faire, de petits modules de formation autour de thématiques importantes ont été élaborées par nos soins et diffusées via un Learning Management System (LMS), Moodle. Nous avons constaté que ces campagnes de sensibilisation ont eu un effet positif sur les utilisateurs.

Mots clés : systèmes d'informations, sécurité numérique, LMS

Abstract

In this increasingly connected world, numerous digital challenges stand before us. Among these, ensuring the security of data within our information systems under all circumstances stands out as one of the most sensitive and important. In order to adequately confront this significant challenge, many measures are put in place such as access control, data encryption, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), awareness, etc. Among these measures, one of the most crucial is digital security awareness.

Our work aims to raise awareness of digital security among users of the Ministry of Urban Development and Transport so that they become informed users and, consequently, a strong line of defence contributing to the security of their organization's data. To achieve this, small training modules on important topics have been developed by us and disseminated via an Learning Management System (LMS), Moodle. We have observed that these awareness campaigns have had a positive effect on users.

Key words: information systems, digital security, LMS

Table des figures

2.1 Installation des paquets nécessaires. 10
2.2 Création de l'utilisateur de la base de données et assignation de ses droits 11
2.3 Modification des permissions au niveau du serveur web 11
2.4 Assignaton des droits aux dossiers web de moodle 11
2.5 Confirmations des chemins 12

3.1 Page d'accueil 16
3.2 Page *Mes cours* 17
3.3 Aperçu du module *Sensibilisation aux mots de passe : Les bonnes pratiques* 17
3.4 Statistiques issues du quiz sur le document scénario (1/2) 18
3.5 Statistiques issues du quiz sur le document scénario (2/2) 19
3.6 Statistiques issues du quiz sur les bonnes pratiques 19
3.7 Statistiques issues du quiz sur les bonnes pratiques du module relatif aux mots de passe (1/2) 20
3.8 Statistiques issues du quiz sur les bonnes pratiques du module relatif aux mots de passe (2/2) 20
3.9 Questionnaire (1/3) 24
3.10 Questionnaire (2/3) 25
3.11 Questionnaire (3/3) 25
3.12 Programme des campagnes de sensibilisation (1/2) 26
3.13 Programme des campagnes de sensibilisation (2/2) 26
3.14 Question 1 posée aux utilisateurs 27
3.15 Question 4 posée aux utilisateurs 27

Liste des tableaux

2.1 Tableau comparatif de quelques LMS existants. 8
2.2 Analyse des risques inhérents aux utilisateurs 13

Liste des acronymes

LMS :

Learning Management System

MCVT :

Ministère du Cadre de Vie et des Transports

PCA :

Plan de Continuité d'Activités

PRA :

Plan de Reprise d'Activités

RAM :

Random Access Memory

Glossaire

Chiffrement de données : processus de conversion des données en un format illisible sans la clé de déchiffrement appropriée. Il est utilisé pour protéger la confidentialité des informations, assurant que même si des données sont interceptées, elles restent inintelligibles sans la clé de déchiffrement

Confidentialité : principe de base en sécurité informatique qui vise à garantir que les informations sont accessibles uniquement aux personnes autorisées

Contrôle d'accès : ensemble de mécanismes et de politiques qui régulent l'accès aux ressources d'un système informatique. Cela implique souvent l'authentification des utilisateurs, l'autorisation des actions spécifiques et la gestion des privilèges pour garantir que seules les personnes autorisées ont accès aux informations ou aux fonctionnalités appropriées

Disponibilité : principe de base en sécurité informatique qui vise à garantir que les informations et les ressources sont accessibles lorsque nécessaire

Ingénierie sociale : méthode utilisée par des individus malveillants pour manipuler et tromper les gens afin d'obtenir des informations confidentielles, d'accéder à des systèmes informatiques ou de compromettre la sécurité d'une organisation. Cela implique souvent la manipulation psychologique des individus plutôt que l'exploitation de failles techniques

Intégrité : principe de base en sécurité informatique qui vise à assurer que les données ne sont ni altérées ni modifiées de manière non autorisée.

PCA : stratégie organisée visant à maintenir les opérations essentielles d'une organisation pendant et après un événement perturbateur. Il englobe souvent la prévention, la préparation, la réponse et la récupération après des incidents.

PRA : stratégie organisée visant à restaurer rapidement les opérations normales après un incident majeur, tel qu'une catastrophe naturelle, une panne de système ou une attaque informatique

RAM : type de mémoire volatile utilisée par les ordinateurs pour stocker temporairement des données et des programmes pendant leur exécution

Traçabilité : fait référence à la capacité de suivre et d'enregistrer les activités et les changements dans un système, permettant ainsi de retracer l'origine, l'évolution et l'impact des actions effectuées

Introduction Générale

Le paysage numérique contemporain a considérablement évolué au cours des dernières décennies, apportant avec lui d'innombrables avantages, mais également de nouveaux défis en matière de sécurité. En particulier, les institutions gouvernementales, et plus précisément le Ministère du Cadre de Vie et des Transports en charge du développement durable (MCVT) sont confrontés à des enjeux cruciaux liés à la protection des informations sensibles dans un monde de plus en plus connecté. Les menaces numériques, qu'elles émanent de cybercriminels, d'acteurs étatiques hostiles ou même d'erreurs humaines, représentent des dangers potentiels pour la sécurité nationale. Face à cette réalité, la nécessité de renforcer la sensibilisation à la sécurité numérique au sein du MCVT devient nécessaire et primordiale.

Problématique

Conformément au code du numérique en République du Bénin, l'adoption de la Politique de Sécurité des Systèmes d'Informations de l'Etat (PSSI-E) en 2021 et sur notre initiative, le Ministère du Cadre de Vie et des Transports a entrepris la mise en place de campagnes de sensibilisation. Ces campagnes, déployées à travers la plateforme Moodle, visent à informer et à éduquer les membres de l'organisation sur les bonnes pratiques en matière de sécurité numérique. Ainsi, comment concevoir, mettre en œuvre et évaluer de manière efficace ces campagnes pour garantir un niveau optimal de sensibilisation et renforcer la protection des données au sein du Ministère ?

Contexte et justificatif

Les structures et les entreprises font face à des risques de sécurité numérique croissants en raison de la dépendance croissante aux technologies de l'information et de la communication. Le Ministère du Cadre de Vie et des Transports qui est responsable de la gestion des infrastructures et des services liés à l'environnement et aux transports n'échappe pas à cette réalité. Dans le cadre de ses responsabilités, le Ministère collecte, stocke et traite une quantité importante de données liées à la mobilité, à l'environnement et à d'autres aspects connexes. Compte tenu de ces risques auxquels il fait face et des conséquences de leur survenue (impossibilité à utiliser les ressources, compromission des données,

divulgation de données, etc.), il est devenu impératif pour ce dernier de renforcer la sensibilisation et la formation de ses employés aux risques liés à la sécurité numérique. Une sensibilisation accrue permettra de réduire les incidents de sécurité, d'améliorer les pratiques de cybersécurité au sein du Ministère et de promouvoir une culture de sécurité où chaque utilisateur est conscient des risques et adopte des comportements sécurisés dans son utilisation des technologies.

Objectifs

L'objectif global de notre travail est d'améliorer la sécurité numérique du MCVT en sensibilisant les employés aux risques et aux bonnes pratiques. A cet effet, nous devons atteindre les objectifs spécifiques suivants :

- identifier les principaux risques de sécurité numérique auxquels sont exposés les utilisateurs du MCVT ;
- concevoir des campagnes de sensibilisation adaptées aux besoins et aux spécificités du MCVT ;
- évaluer l'impact de la campagne de sensibilisation mise en place en collectant des données sur la participation des utilisateurs, en menant des enquêtes ou des simulations pour évaluer les changements de comportement ;

Organisation du mémoire

Notre travail est composé de trois chapitres. Le premier est consacré à une revue de littérature sur la sécurité numérique, la sensibilisation à la sécurité numérique et les LMS. Le deuxième chapitre est dédié au choix du LMS utilisé et à la mise en place des campagnes de sensibilisation. Le dernier chapitre, quant à lui, est chargé de montrer les résultats obtenus suite auxdites campagnes et des perspectives.

Chapitre 1

Revue de Littérature

Introduction

La révolution numérique a transformé notre façon de vivre, de travailler et de communiquer, apportant avec elle une myriade d'opportunités tout en exposant simultanément des vulnérabilités considérables. Au cœur de cette ère numérique, la sécurité numérique émerge comme un impératif essentiel, particulièrement pour des institutions stratégiques telles que le Ministère du Cadre de Vie et des Transports en charge du Développement Durable. Ce premier chapitre se consacre à une revue de littérature approfondie, explorant les notions de sécurité numérique et de Learning Management System (LMS).

1.1 Sécurité numérique

Dans cette section, nous verrons ce que c'est que la sécurité numérique et ses enjeux.

1.1.1 Qu'est ce que la sécurité numérique ?

La sécurité numérique, englobe l'ensemble des mesures, des stratégies et des technologies mises en place pour protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les menaces et les attaques numériques. Elle vise à assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations dans un environnement numérique [1]. La sécurité numérique s'étend à la protection contre les logiciels malveillants, les violations de données, l'ingénierie sociale et d'autres formes d'activités malveillantes.

1.1.2 Enjeux de la sécurité numérique

- **Protection des données sensibles** : Les organisations traitent une quantité importante de données sensibles, qu'il s'agisse d'informations client, de données financières, de propriété intellectuelle ou d'autres informations confidentielles. La perte ou la compromission de ces données peut avoir des conséquences graves telles que des atteintes à la vie privée, des pertes financières et des dommages à la réputation.

- **La continuité de l'activité** : les systèmes informatiques sont aujourd'hui indispensables au bon fonctionnement de la plupart des structures. Une cyberattaque peut perturber ou paralyser ces systèmes, entraînant des pertes de productivité et des coûts importants. La disponibilité continue desdits systèmes est cruciale pour le bon fonctionnement d'une organisation.
- **Conformité réglementaire** : de nombreuses structures sont soumises à des obligations réglementaires en matière de sécurité des données. Une violation de ces obligations peut entraîner des sanctions financières importantes [2].

1.2 Sensibilisation à la sécurité numérique

La sensibilisation à la sécurité numérique désigne l'ensemble des activités éducatives, informatives et de communication visant à accroître la conscience et la compréhension des utilisateurs concernant les risques liés à la sécurité numérique. Cette démarche vise à changer les comportements en encourageant les bonnes pratiques de sécurité, en réduisant les erreurs humaines et en renforçant la résilience des individus et des organisations face aux menaces numériques.
Pour faire de la sensibilisation à la sécurité numérique, on peut opter pour une approche physique avec l'utilisation d'affiches, de flyers, l'organisation de meetings, etc ; et pour une approche digitale avec des supports numériques tels que des documents et des vidéos. Ici, nous avons opté pour une approche digitale et avons comme outil de diffusion des supports, un LMS [3].

1.3 Learning Management System (LMS)

1.3.1 Qu'est ce qu'un LMS ?

Un Learning Management System (Système de Gestion de l'Apprentissage en français) est une plateforme logicielle conçue pour faciliter la gestion, la diffusion et le suivi des programmes de formation en ligne. Les LMS offrent des fonctionnalités telles que la création de cours, la distribution de contenu pédagogique, la gestion des inscriptions, le suivi des progrès des apprenants, l'évaluation des performances et la génération de rapports. Ces systèmes sont largement utilisés dans les contextes éducatifs, corporatifs et institutionnels pour offrir des expériences d'apprentissage flexibles, interactives et efficaces, notamment dans le cadre de programmes de sensibilisation à la sécurité numérique.

1.3.2 Avantages et Inconvénients à l'utilisation d'un LMS

- **Avantages**
  - **Accessibilité** : les LMS offrent une plateforme centralisée, permettant un accès facile aux cours et aux ressources pédagogiques de n'importe où, favorisant ainsi l'apprentissage à distance.
  - **Suivi des Progrès** : les fonctionnalités de suivi des progrès permettent aux enseignants et aux administrateurs de suivre les performances des apprenants, d'identifier les domaines qui nécessitent une attention particulière et d'ajuster les stratégies d'enseignement en conséquence.

  - **Gestion des Contenus** : les LMS facilitent la création, la gestion et la distribution de contenu pédagogique varié, favorisant une expérience d'apprentissage riche et interactive.
  - **Personnalisation de l'Apprentissage** : (Si disponible) les LMS permettent une personnalisation des parcours d'apprentissage, s'adaptant ainsi aux besoins individuels des apprenants.

- **Inconvénients**
  - **Complexité Initiale** : la mise en place d'un LMS peut être complexe, nécessitant des ressources importantes en termes de temps, de formation et de configuration.
  - **Coûts** : les coûts initiaux et de maintenance d'un LMS peuvent être substantiels, en particulier pour les petites organisations ou les établissements éducatifs avec des budgets limités.
  - **Dépendance Technologique** : une dépendance excessive à la technologie peut entraîner des problèmes en cas de pannes systèmes, de problèmes de connectivité ou d'obsolescence des plateformes.
  - **Résistance au Changement** : certains utilisateurs, en particulier ceux moins familiers avec les technologies, peuvent résister au passage à un environnement d'apprentissage en ligne, affectant la réussite de l'adoption du LMS [4].

Conclusion

De cette revue de littérature, il apparaît clairement que la sécurité numérique est un impératif majeur, particulièrement pour des institutions aussi sensibles que les structures étatiques dont le MCVT. Les fondements théoriques ont été explorés, démontrant que la sécurité numérique ne se limite pas à des considérations techniques, mais s'étend également à des dimensions stratégiques. Les menaces émergentes exigent une réponse proactive et holistique. La sensibilisation à la sécurité numérique se présente comme une composante essentielle, visant à transformer les utilisateurs en maillons forts de la cybersécurité. Dans le prochain chapitre, nous explorerons la démarche avec laquelle nous avons réaliser le choix de notre LMS et celle concernant la confection des campagnes de sensibilisation.

Chapitre 2

Choix, installation du LMS et mise en place des campagnes de sensibilisation

Introduction

Le déploiement efficace de campagnes de sensibilisation à la sécurité numérique au sein du MCVT repose sur deux éléments essentiels : le choix judicieux du Learning Management System (LMS) et la conception des campagnes elles-mêmes. Dans ce chapitre, nous explorerons ces aspects cruciaux du renforcement de la culture de sécurité au sein de la structure. La première section se penchera sur le processus de sélection du LMS à utiliser. Puis la seconde abordera son installation. Enfin, la troisième abordera les étapes suivies au cours du processus de conception des campagnes de sensibilisation et de la stratégie de promotion des campagnes à l'endroit des utilisateurs.

2.1 Choix du LMS

2.1.1 Critères retenus pour le choix du LMS

Après des discussions avec nos encadreurs, nous avons opté, afin de choisir un LMS répondant à nos besoins, de nous baser sur les critères qui suivent :

- déployable localement
- open source
- facile à administrer
- intégrant des fonctionnalités de suivi et de statistiques
- mises à jour régulières
- documentation complète et communauté active

2.1.2 Etude comparative de quelques LMS

Le marché regorge de nombreux LMS basés sur le web ou sur le Cloud, freemium ou payant. Au nombre de ceux-ci, nous pouvons citer : Moodle, FormaLMS, CanvasLMS, Atutor, iSpringLearn, SkyPrep, Adobe Captivate Prime, TalentLMS, etc. Le Tableau 2.1 ci-après récapitule les avantages et les inconvénients de quelques solutions.

TABLEAU 2.1 : Tableau comparatif de quelques LMS existants.

Solutions	Avantages	Inconvénients	Score
Moodle	• Open Source et déployable localement • Communauté très active • Grande flexibilité et capacité de personnalisation • Grande capacité d'extension des fonctionnalités grâce aux nombreux plugins disponibles • Prise en charge de nombreux types de contenu (dont les contenus interactifs) • Suivi des progrès des utilisateurs • Documentation détaillée et compréhensible	• Maintenance à faire régulièrement	6
FormaLMS	• Open Source et déployable localement • Interface utilisateur moderne • Communauté active • Rapports et statistiques détaillés	• Peu de plugins tiers • Documentation moins exhaustive	4.5
CanvasLMS	• Open source et déployable localement • Interface utilisateur intuitive et conviviale • Rapports d'activités bien faits	• Peu d'options de personnalisation • Assez de fonctionnalités clés non open-source	4
Atutor	• Open Source et déployable localement • Interface utilisateur adaptable • Suivi des progrès	• Moins de fonctionnalités avancées • Mises à jour peu fréquentes • Documentation limitée et communauté peu active	4

SkyPrep	• Interface utilisateur intuitive • Personnalisation facile des cours • Rapports et suivi de performances	• basé sur le cloud • Personnalisation limitée de l'interface • Coûteux (montant disponible qu'après discussion avec un expert)	4
Adobe Captivate Prime	• Interface intuitive • Flexibilité dans la création de contenu • Personnalisation du parcours d'apprentissage • Rapports et analyses approfondis	• Coûteux (4$/mois/utilisateur avec une réduction pour les entreprises ayant plus de 500 utilisateurs) • Dépendance à l'écosystème Adobe	4
TalentLMS	• Interface utilisateur intuitive • Mises à jour automatiques • Fonctionnalités de reporting avancées • Personnalisation facile des contenus	• basé sur le cloud • Coûteux (à partir de 69$ le mois) • Personnalisation limitée de l'interface • Fonctionnalités avancées nécessitant des frais.	4
iSpringLearn	• Interface utilisateur intuitive • Fonctionnalités de suivi de progrès • Rapports et analyses avancés	• basé sur le cloud • Coûteux (fonction du nombre d'utilisateurs, pour 100 utilisateurs, 2.87$ par mois facturé annuellement) • Personnalisation limitée de l'interface • Dépendance à iSpring Suite	4

A ces avantages et inconvénients s'ajoute un score (cf Tableau 2.1) déterminé par la satisfaction des critères que nous avons énoncé plus haut. A cet effet, un critère satisfait confère 1 point. Nous avons remarqué que seul un outil satisfait l'intégralité de nos critères, Moodle. D'où notre choix.

2.2 Mise en place de la plateforme LMS

Comme nous l'avons dit plus haut, nous avons choisi d'utiliser la plateforme Moodle comme plateforme d'apprentissage pour les utilisateurs. Dans le cadre de son installation, Moodle donne les recommandations que voici :

- Espace disque : 5 Go minimum
- Processeur : 1 GHz minimum
- Mémoire RAM : 1 Go ou plus
- Système d'exploitation : Windows ou Linux [5]

Après discussion avec nos encadreurs, il a été retenu que la plateforme soit mise en place sur un environnement Linux, plus précisément sous Ubuntu et sur une machine virtuelle dont les caractéristiques sont :

- Espace disque : 25 Go

- Processeur : 2,6 GHz
- Mémoire RAM : 3 Go

La version de Moodle utilisée est la 4.3.2+ qui était la plus à jour au moment de l'exécution de notre travail.
Voici les différentes étapes de la mise en place de la plateforme Moodle [6] :

- **Installation des paquets nécessaires**
  A cette étape, il nous faut installer les paquets nécessaires pour apache, mysql et php (cf Figure 2.1).



FIGURE 2.1 : Installation des paquets nécessaires.

- **Configuration du serveur web**
  A cette étape, nous devons apporter des modifications au fichier de configuration de php du serveur web, *php.ini*. Plus précisément, nous devons successivement :

  1. décommenter la ligne commençant par **`max_input_vars`** et augmenter sa valeur à 5000
  2. augmenter la valeur du paramètre **`upload_max_filesize`** à 20M
  3. augmenter la valeur du paramètre **`max_file_uploads`** à 40
  4. vérifier le fonctionnement du serveur web en entrant l'adresse IP de la machine dans un navigateur web (Si ça fonctionne, une page propre au serveur web apache devrait vous le notifier)

- **Téléchargement de Moodle**
  Il faut télécharger Moodle. Dans notre cas, nous l'avons fait depuis le site officiel de Moodle, `https://www.moodle.org`. Après téléchargement, il faut l'extraire dans le dossier /var/www/html.

- **Configuration de la base de données**
  A cette étape, nous devons :

  1. démarrer mysql avec la commande **sudo service mysql start**

  2. créer la base de données pour moodle avec la commande : **CREATE DATABASE dbmoodle DEFAULT CHARACTER SET utf8mb4 COLLATE `utf8mb4_unicode_ci`;**

  3. créer un utilisateur pour la base de données à l'aide de la commande **CREATE USER 'moodleuser'@'localhost' IDENTIFIED BY 'motdepasse';**

  4. assigner des droits à l'utilisateur à la base de données de moodle (cf Figure 2.2).

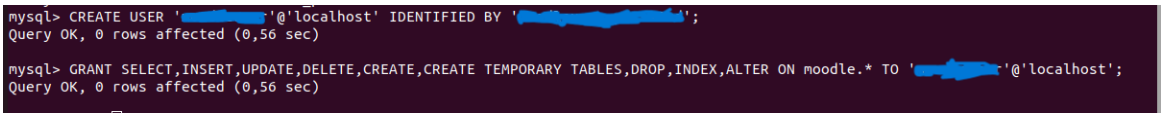


FIGURE 2.2 : Création de l'utilisateur de la base de données et assignation de ses droits

La création de l'utilisateur et l'assignation de ses privilèges sur la base de données ont été réalisées avec succès conformément à la capture ci-dessus.

- **Définition des permissions au niveau du serveur web**
  Pour ce faire, il faut :

  1. modifier les permissions pour le serveur web (cf Figure 2.3) ;

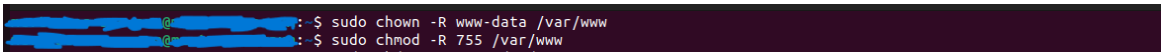


FIGURE 2.3 : Modification des permissions au niveau du serveur web

La Figure 2.3 montre que les permissions ont bien été modifiées.

  2. créer un dossier pour les données moodle avec la commande **sudo mkdir /var/moodledata** ;

  3. assigner des droits aux dossiers web de moodle (cf Figure 2.4).

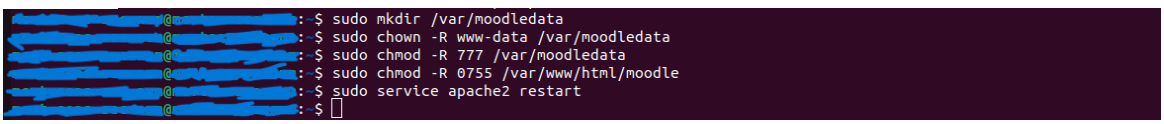


FIGURE 2.4 : Assignaton des droits aux dossiers web de moodle

Les droits ont bien été assignés, conformément à la Figure 2.4.

- Installation de Moodle

1. aller sur un navigateur web à l'adresse `http://adresse_ip/moodle` et choisir la langue ;

2. confirmer les chemins (cf Figure 2.5) menant au site web de Moodle, à son dossier sur le serveur et au dossier de données ;

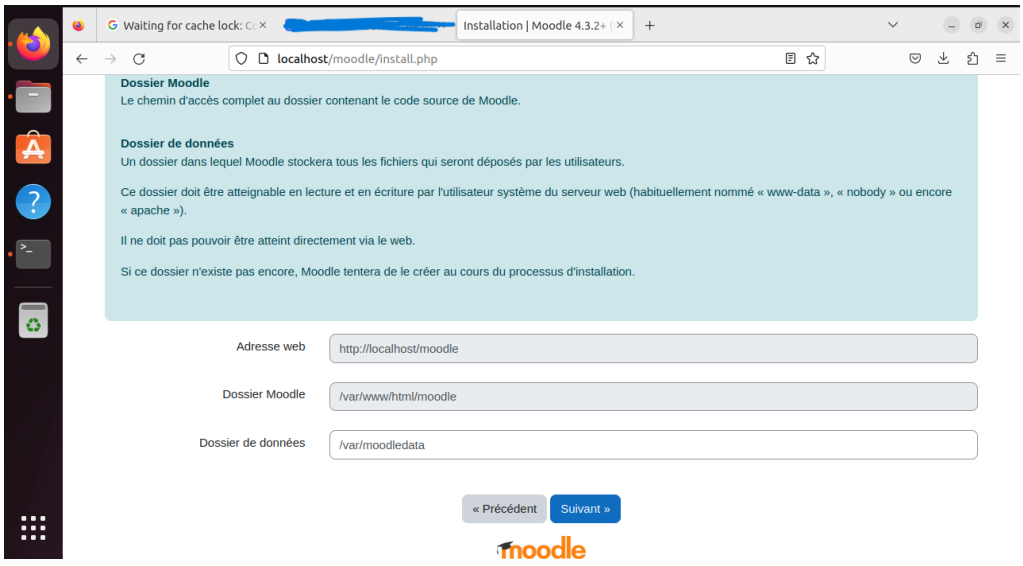


FIGURE 2.5 : Confirmations des chemins

3. choisir le pilote de la base de données (dans notre cas, il s'agit de *MySQL amélioré*) ;

4. paramétrer la base de données ;

5. installer moodle ;

6. paramétrer le compte administrateur ;

7. effectuer les réglages de la page d'accueil.

Après cette dernière étape, l'installation est terminée. Nous n'avons pas détaillé l'installation de Moodle compte tenu du fait qu'il ne s'agit pas du sujet principal ici. Pour plus de détails dans le processus de mise en place, vous pouvez consulter : `https://towios.vivaldi.net/moodle-ubuntu-install/`

2.3 Conception des campagnes de sensibilisation

2.3.1 Echantillonnage de la population constituant les utilisateurs

Avant de penser à mettre en place les modules de sensibilisation, il fallait d'abord savoir si cette sensibilisation allait impliquer tous les utilisateurs du Ministère. Après discussion avec nos encadreurs, compte tenu du fait qu'il s'agissait de la première fois que nous mettons sur pied un tel projet, nous avions jugé judicieux de n'utiliser qu'un échantillon avant d'impliquer toute la population. Pour effectuer cet échantillonnage, nous avons utilisé la technique d'*échantillonnage en grappes* [7]. Nous nous sommes basé sur les directions composant le Ministère et avons prélevé les utilisateurs au niveau de chaque direction de sorte à avoir 20% de la population totale suivant la règle de Pareto (cette règle stipule que 20% d'une population peut fournir 80% des résultats de cette dernière [8]). Sur une population de 105 utilisateurs recensés, 21 ont été sélectionnés. Il est à noter que les 105 utilisateurs recensés ne représentent pas la population totale des utilisateurs du Ministère. Le recensement s'est basé sur les utilisateurs qui étaient sur place (pas dans des structures détachées du Ministère), en poste (pas en congés) et qui n'étaient pas susceptibles de se déplacer (missions) au cours de la période de sensibilisation.

2.3.2 Analyse des besoins en matière de sécurité numérique des utilisateurs

Après avoir prélevé notre échantillon, il était impératif de comprendre les besoins spécifiques des utilisateurs le composant. Pour ce faire, nous avons effectué une petite analyse de risques à travers un questionnaire. Ce dernier a été conçu dans le but non seulement d'avoir un aperçu du niveau de connaissance général des utilisateurs sur la sécurité numérique, mais aussi des comportements liés à cette dernière qu'ils adoptent quotidiennement. A cet effet, nous avons élaboré des questions 3.11 liées aux risques propres au facteur humain les plus courants.
Dans l'optique que les réponses à ce questionnaire soient fiables, nous avons opté pour une réponse physique et non en ligne. Ainsi, nous sommes passés dans le bureau de chaque utilisateur présent dans l'échantillon, lui avions présenté le questionnaire et chacun y a répondu devant nous. Suite au remplissage de ce formulaire, voilà l'analyse que nous en avons faite (cf Tableau 2.2) :

TABLEAU 2.2 : Analyse des risques inhérents aux utilisateurs

Point de Vulnérabilité	**Pourcentage des utilisateurs concernés**	**Risque**
Compréhension faible de la sécurité numérique	40%	Les utilisateurs mal informés sont plus susceptibles de tomber dans des pièges en ligne, de divulguer des informations sensibles et de ne pas reconnaître les signaux d'alerte liés à la sécurité.
Réutilisation de mots de passe	60%	L'utilisation de mots de passe identiques accroît le risque de compromission multiple en cas de violation d'un compte. Un seul compte piraté peut entraîner la compromission de plusieurs comptes en ligne.

Absence de gestionnaire de mots de passe	100%	La non utilisation d'un gestionnaire de mots de passe n'est pas problématique, nous trouvons d'ailleurs que c'est mieux ainsi.
Réception de messages ou appels suspects	10%	Les escrocs ciblant les utilisateurs peuvent obtenir des informations personnelles précieuses en se faisant passer pour des organismes officiels.
Manque de méfiance envers les liens et pièces jointes	20%	Cliquer sur des liens ou des pièces jointes provenant de sources inconnues peut entraîner l'installation de logiciels malveillants ou la redirection vers des sites de phishing.
Méconnaissance pour reconnaître un site légitime	60%	Les utilisateurs peuvent être victimes de sites de phishing qui ressemblent à des sites légitimes, conduisant ainsi à la divulgation d'informations sensibles.
Partage imprudent d'informations personnelles sur les réseaux sociaux	40%	Le partage imprudent d'informations personnelles peut conduire à l'usurpation d'identité, au harcèlement en ligne ou à d'autres formes d'exploitation.

2.3.3 Choix des thématiques des campagnes et mise au point du programme

Suite à l'analyse précédente (cf Tableau 2.2), nous avons opté pour les thématiques suivantes :

- **Gestion de mots de passe** : cette thématique a été chosie dans l'optique d'apprendre aux utilisateurs les bonnes pratiques en ce qui concerne non seulement la création de mots de passe forts mais aussi comment les gérer.
- **Navigation internet et sécurité des e-mails** : ici, l'objectif est de montrer aux utilisateurs dans un premier temps les risques liés à une navigation internet imprudente puis les bonnes pratiques à observer et dans un second temps, les bonnes habitudes en ce qui concerne les mails reçus.
- **Sécurité des données et des appareils** : avec cette thématique, nous cherchons à sensibiliser les utilisateurs en ce qui concerne la sécurité de leurs appareils en général et de leurs données personnelles en particulier.

Pour visualiser le programme en détail, voir figure 3.13 .

2.3.4 Confection des modules de sensibilisation

Pour ces campagnes, nous avons élaborés des supports document de deux types :

- un document-scénario : qui est en réalité un scénario imaginé sous forme de dialogue mettant en scène le risque sur lequel on veut baser la sensibilisation et ses conséquences. Pour le réaliser, nous imaginons un scénario, examinons sa pertinence puis le mettons en page. Ce document doit permettre à l'utilisateur de visualiser concrètement le risque et ses conséquences afin de prendre conscience de l'impact que pourraient avoir des comportements peu sûrs et, de ce fait, la nécessité d'adopter des pratiques sûres ;
- un document-recommandations : qui est un ensemble de bonnes pratiques, de recommandations liées au risque abordé. Pour son élaboration, on passe d'abord par une phase de recherches

afin d'apporter le plus d'informations utiles. Nous les trions ensuite et prenons les plus pertinentes pour les utilisateurs et les mettons sous forme de document. Ce document doit servir de guide aux utilisateurs en ce qui concerne les bonnes pratiques à avoir. En principe, après la lecture de ces dernières, l'utilisateur fait un pas assuré vers l'objectif visé, renforcer la prudence de ces utilisateurs.

Afin d'évaluer les utilisateurs, nous avons pensé à utiliser des quiz. Ils peuvent comprendre des QCU (Question à Choix Unique) ou des questions Vrai/Faux. Ainsi, deux types de quiz sont présents dans nos campagnes :

- un quiz post document-scénario : ce quiz nous permet de nous assurer que les utilisateurs ont bel et bien lu le document scénario et qu'ils ne l'ont juste pas ouvert. Ainsi, dans les questions, au moins une est basée sur des détails qui paraissent insignifiants au prime abord tels que le décor ou les lieux où se déroulent les scènes ;
- un quiz post document-recommandations : ici, il s'agit de voir si les utilisateurs ont assimilé les bonnes pratiques qu'ils viennent de lire. Les questions du quiz incorporent des questions de compréhension sur les bonnes pratiques reçues et des questions qui nécessitent d'appliquer ces bonnes pratiques dans un contexte donné.

2.3.5 Stratégie de promotion des campagnes auprès des utilisateurs

Dans le but de promouvoir cette campagne, nous nous sommes assurés d'attiser l'intérêt des utilisateurs en ce qui concerne la sécurité numérique lors de la remise du formulaire à remplir. Tous étaient d'avis du bien fondé de mettre en place une telle initiative et nous ont vivement encouragé. De plus, deux fois par semaine, nous envoyons un mail de rappel aux participants.

Conclusion

Au sein de ce chapitre, il a été question de présenter comment s'est opéré le choix de notre LMS, de sa mise en place ainsi que de savoir comment les campagnes de sensibilisation ont été mises en place. Dans le prochain chapitre, il sera donc question d'apprécier les résultats de notre démarche et d'en discuter.

Chapitre 3

Résultats

Introduction

Dans cette section, nous présentons d'abord la plateforme obtenue, puis l'impact de notre campagne sur les utilisateurs, pour finir par nos perspectives en ce qui concerne une amélioration envisageable pour notre travail.

3.1 Présentation de la plateforme

Après installation, modification et mise en place des campagnes, voici un aperçu (cf Figure 3.1) de la plateforme via quelques pages. En premier lieu, la page d'accueil.

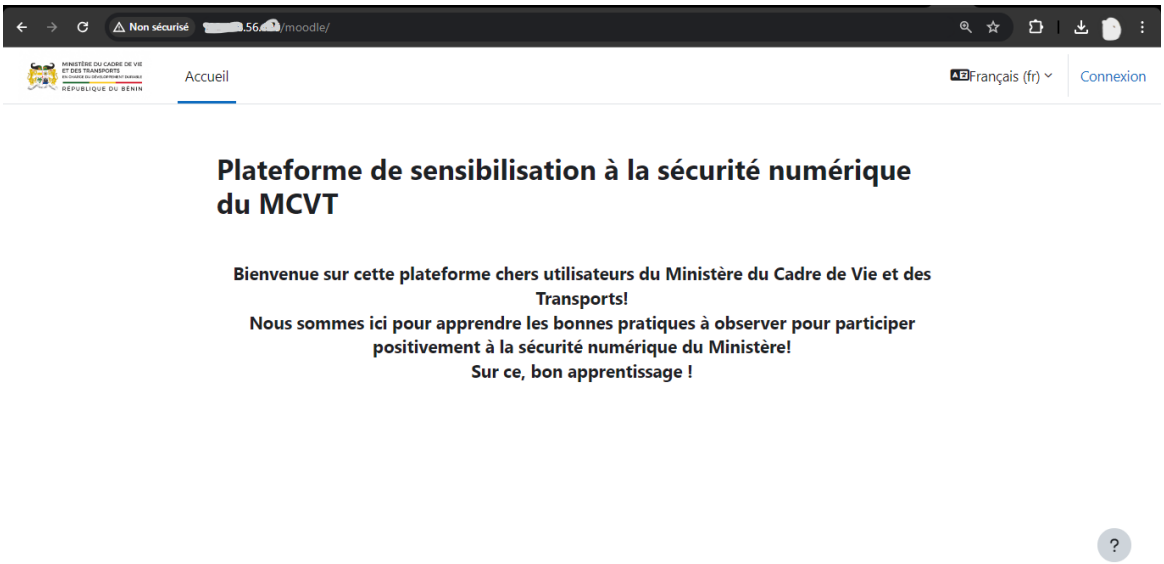


FIGURE 3.1 : Page d'accueil

Puis, la page réservée à la vue d'ensemble des cours disponibles (cf Figure 3.2).

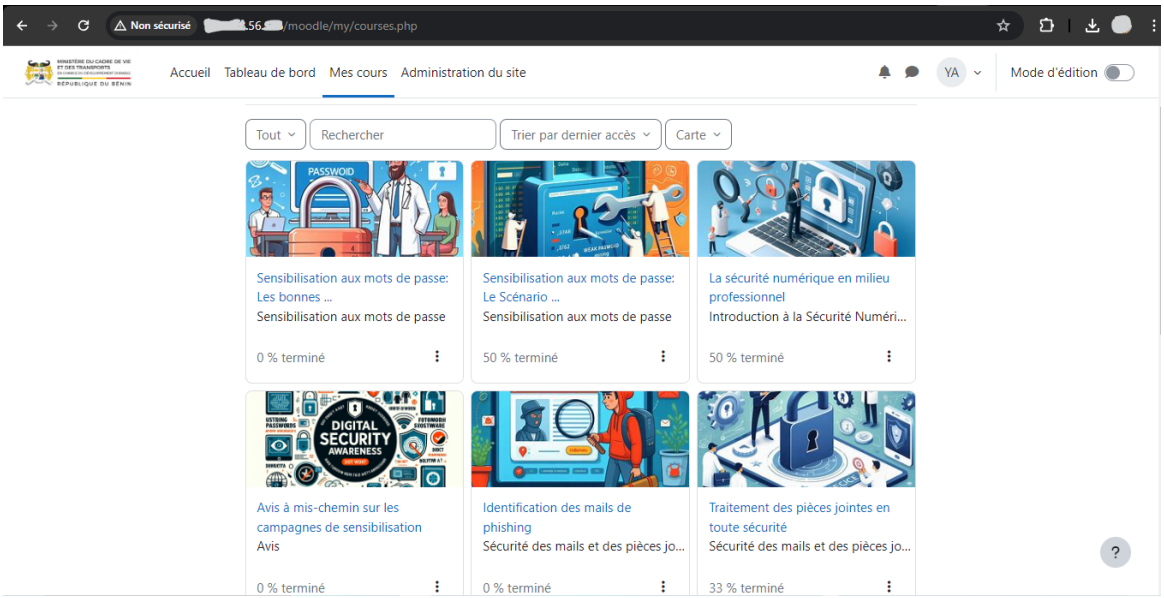


FIGURE 3.2 : Page *Mes cours*

Et enfin, un aperçu de la présentation d'un de nos modules de cours, en occurence, du module ***Sensibilisation aux mots de passe : Les bonnes pratiques*** (cf Figure 3.3).

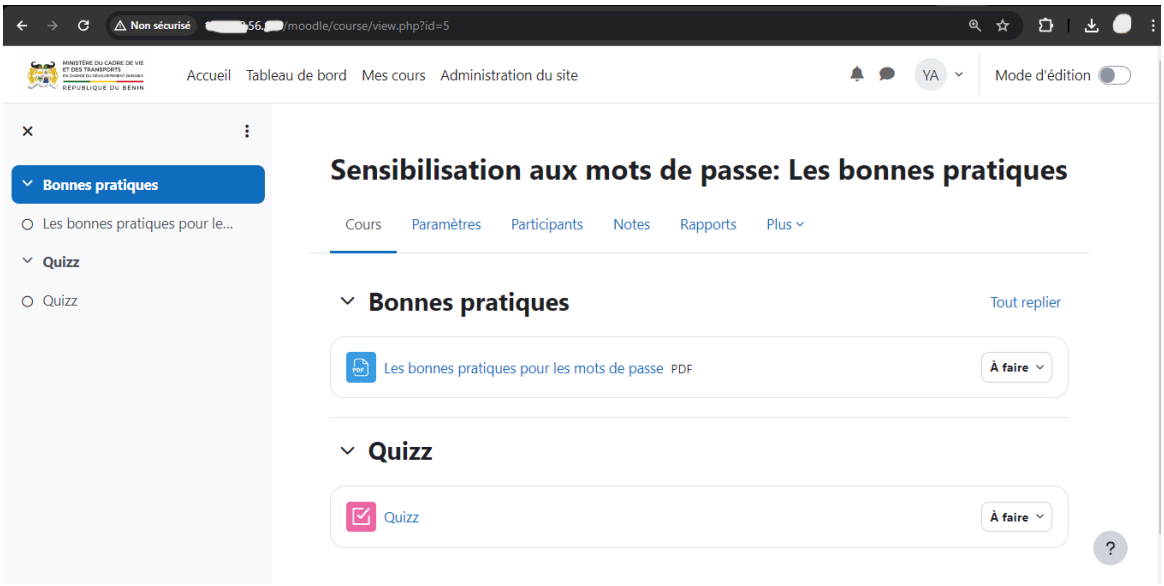


FIGURE 3.3 : Aperçu du module *Sensibilisation aux mots de passe : Les bonnes pratiques*

3.2 Analyse des indicateurs de performance

Pour faire une évaluation de nos campagnes, nous avions prévu analyser trois indicateurs de performance :

- le taux de participation ;
- la compréhension des utilisateurs via les résultats des quiz ;
- les changements de comportements.

3.2.1 Le taux de participation

Comme nous l'avons dit plus haut, 21 participants ont participé à nos campagnes et tous ont commencé par suivre les modules de cours sur la plateforme. Nous avons donc un taux de participation maximal.

3.2.2 La compréhension des utilisateurs

Dans le cadre de l'évaluation de la compréhension des utilisateurs, nous avons prévu des quiz auxquels ces derniers répondent au fur et à mesure que les modules se succèdent. Aussi, nous avons donné la possibilité aux utilisateurs de passer le quiz une seconde fois parce que la validation du quiz n'est possible qu'à l'obtention de la note maximale (20/20). Pour illustrer cette section, nous allons nous baser sur les statistiques des quiz des modules de cours relatifs à la sensibilisation à l'utilisation des réseaux Wi-Fi publics et des mots de passe.

- Module relatif à la sensibilisation sur les réseaux Wi-Fi publics (cf Figure 3.4)

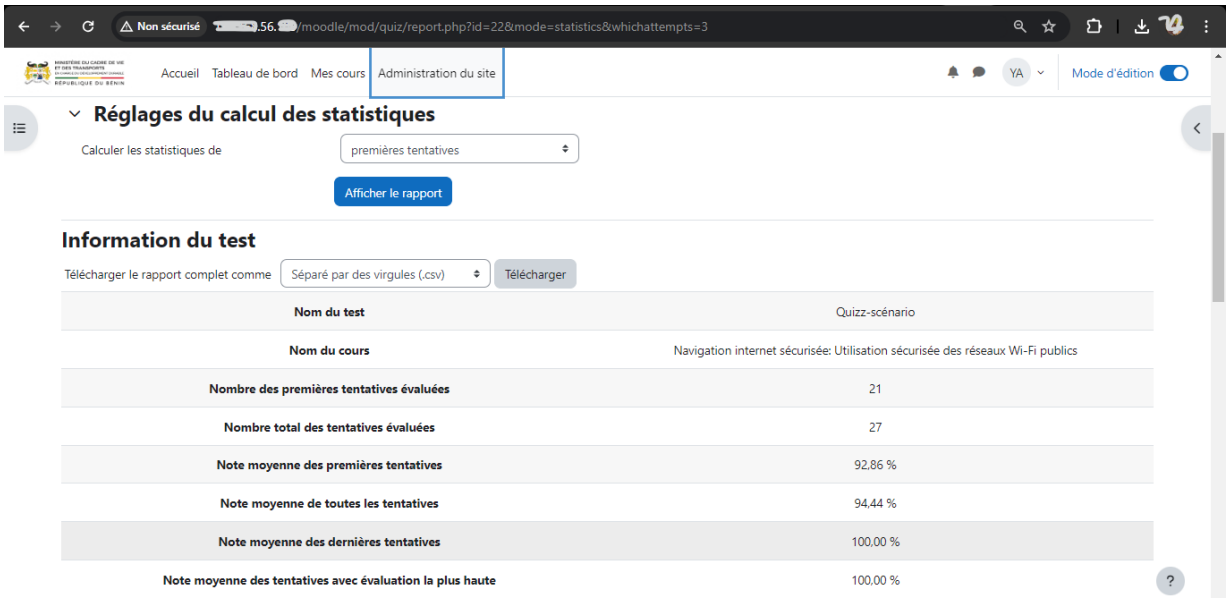


FIGURE 3.4 : Statistiques issues du quiz sur le document scénario (1/2)

Les valeurs qui nous intéressent au niveau de la Figure 3.4 sont : *nombre des premières tentatives évaluées* et *note moyenne des premières tentatives*. Comme leur nom l'indique, elles représentent respectivement le nombre de premières tentatives au quiz et le pourcentage des points obtenus sur l'ensemble de ces premières tentatives. Sur cette capture, on note que 21 premières tentatives ont été enregistrées pour un pourcentage de 92.86% de points récoltés. Ce pourcentage indique que 6 utilisateurs ont raté le quiz à leur première tentative en ratant une question.

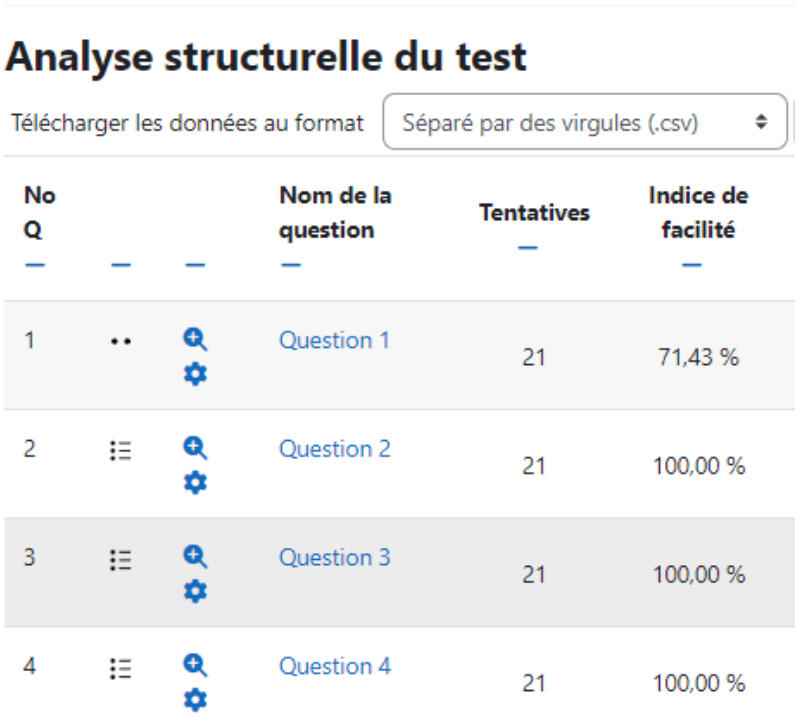


FIGURE 3.5 : Statistiques issues du quiz sur le document scénario (2/2)

La Figure 3.5 présente les statistiques du quiz basées sur l'indice de facilité de chaque question la composant. De cette Figure, on remarque que c'est la question *Question 1* 3.14 qui a posé problème auxdits utilisateurs. Il s'agissait d'une question vrai/faux piège nous permettant de nous faire une idée sur la qualité de la lecture de l'utilisateur. Rater cette question implique ne pas avoir assez fait attention aux détails et suggère une lecture inattentive.

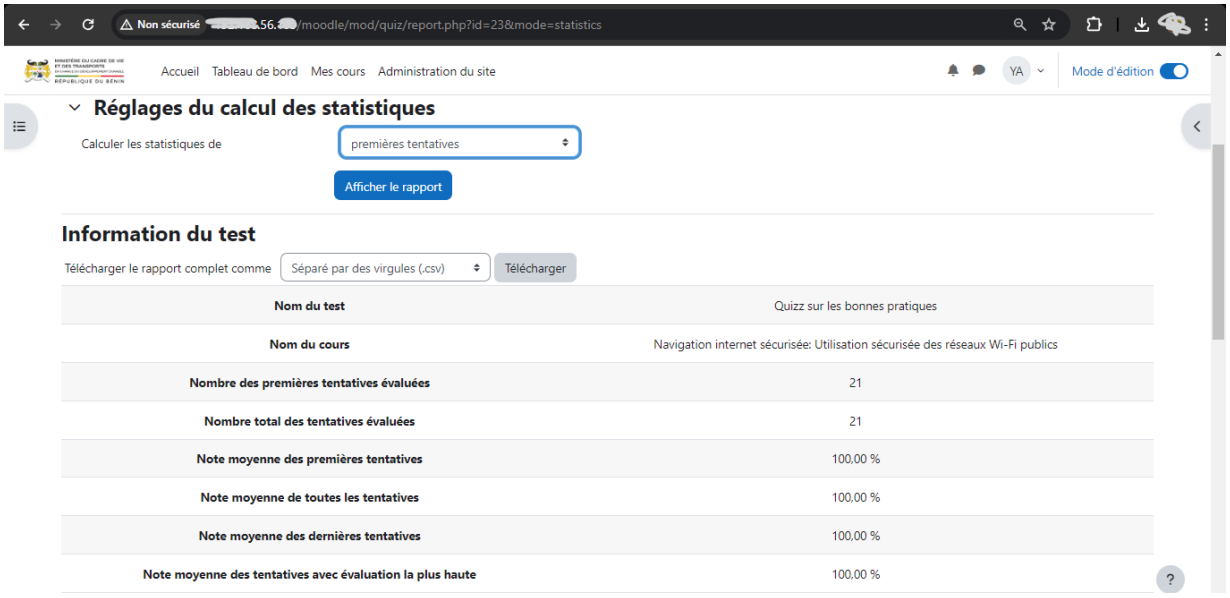


FIGURE 3.6 : Statistiques issues du quiz sur les bonnes pratiques

En ce qui concerne l'évaluation sur les bonnes pratiques pour ce module de cours, on remarque suivant ce que nous montre la Figure 3.6 que tous les utilisateurs ont réussi leur quiz du premier coup. Ce qui veut dire, normalement, que le message est bien passé.

- Module relatif à la sensibilisation aux mots de passe (cf Figure 3.7)

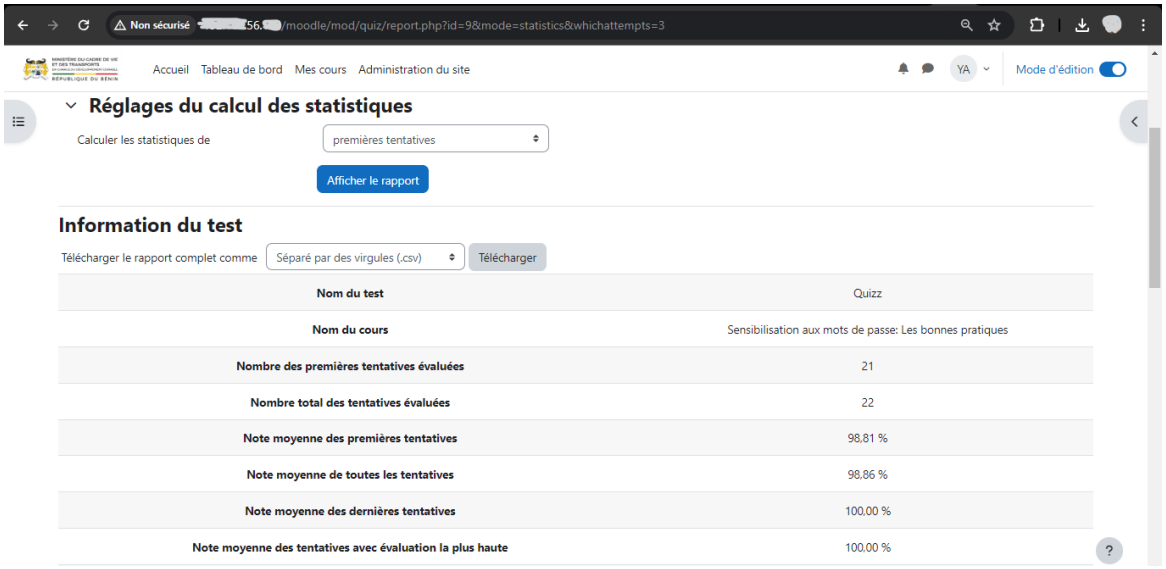


FIGURE 3.7 : Statistiques issues du quiz sur les bonnes pratiques du module relatif aux mots de passe (1/2)

La Figure 3.7 nous montre que 98.81% des points ont été obtenus sur les 21 premières tentatives. Ce pourcentage correspond à un échec dû à une mauvaise réponse d'un utilisateur.

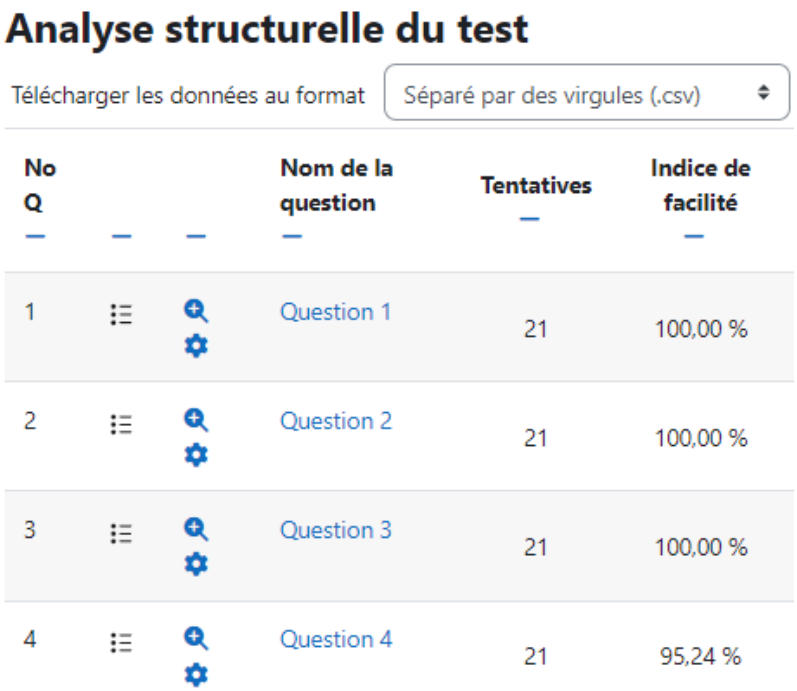


FIGURE 3.8 : Statistiques issues du quiz sur les bonnes pratiques du module relatif aux mots de passe (2/2)

De la Figure 3.8, on remarque que la question que l'utilisateur a raté est *Question 4* 3.15. Il s'agissait d'une question nécessitant l'application des bonnes pratiques données un peu plus haut. Rater cette question peut être dû à deux facteurs :

1. l'utilisateur n'a pas compris : Dans ce cas, une relecture du document devrait suffire. Dans le cas contraire, de plus amples explications via un module informatif est possible. Ce module ne sera disponible que pour cet utilisateur.
2. l'utilisateur n'a pas fait attention au choix de réponse : Il se peut que l'utilisateur ait compris et qu'il ait tout simplement choisi la mauvaise réponse suite à une confusion.

Les deuxièmes tentatives n'ont pas été prises en compte parce que jusqu'à présent, le taux est de 100% de réussite.

3.2.3 Les changements de comportement

Ici, nous avions prévu d'observer et de relever à chaque fois que possible les comportements des utilisateurs. Pour effectuer ces observations, nous avions chargé les Helpdesk de vérifier si les utilisateurs mettent en pratique ce qu'ils lisent, comprennent. En effet, il nous avait été donné de constater que certains utilisateurs notaient leurs mots de passe dans des blocs-notes qu'ils laissent sur leur bureau, sur des fiches qu'ils collent sur l'écran de leur ordinateur de bureau. Aussi, il arrivait que certains laissaient les agents Helpdesk créer les mots de passe pour eux. Ainsi, nous avons demandé aux agents Helpdesk depuis que le programme a débuté de prêter attention à ces comportements et de vérifier s'il y a du changement. Il nous a été révélé que c'était le cas. Les utilisateurs s'appliquent à :

- créer/changer leurs mots de passe convenablement et ne les notent plus à la vue de tous ;
- dissocier les communications privées de celles professionnelles.

On peut donc dire que le programme a eu un impact sur les utilisateurs.
Mais, notre travail n'étant pas parfait, des recommandations ont été formulées par les utilisateurs.

3.3 Perspectives

Dans l'optique d'améliorer notre travail, nous avons pensé à :

- intégrer du contenu multimédia comme des vidéos, des infographies animées ;
- mettre en place des banques de questions afin de diversifier les quiz d'un utilisateur à l'autre ;
- inclure des sessions en temps réel au cours desquelles les utilisateurs pourront interagir de vive voix avec nous ;
- mettre en place un système de récompenses aux utilisateurs qui suivent activement le programme et démontrent une bonne compréhension des notions transmises ;
- si possible, essayer de personnaliser le programme afin que chaque utilisateur puisse avoir un programme propre à ses besoins ;
- effectuer une ou plusieurs simulations de phishing.

Conclusion

Dans ce chapitre, nous avons présenté les résultats de nos campagnes à travers des indicateurs de performance. Il en est ressorti que lesdites campagnes ont permis aux utilisateurs pilotes du MCVT de faire un pas vers l'idéal recherché qui est d'être des utilisateurs informés, conscients des risques qui pèsent sur eux et, par conséquent, de se comporter de la meilleure des manières au quotidien afin d'être une ligne de défense forte pour la sécurité du système d'informations du MCVT. Par contre, notre travail n'étant pas parfait, des perspectives à mettre en œuvre ont été identifiées afin de le rendre meilleur.

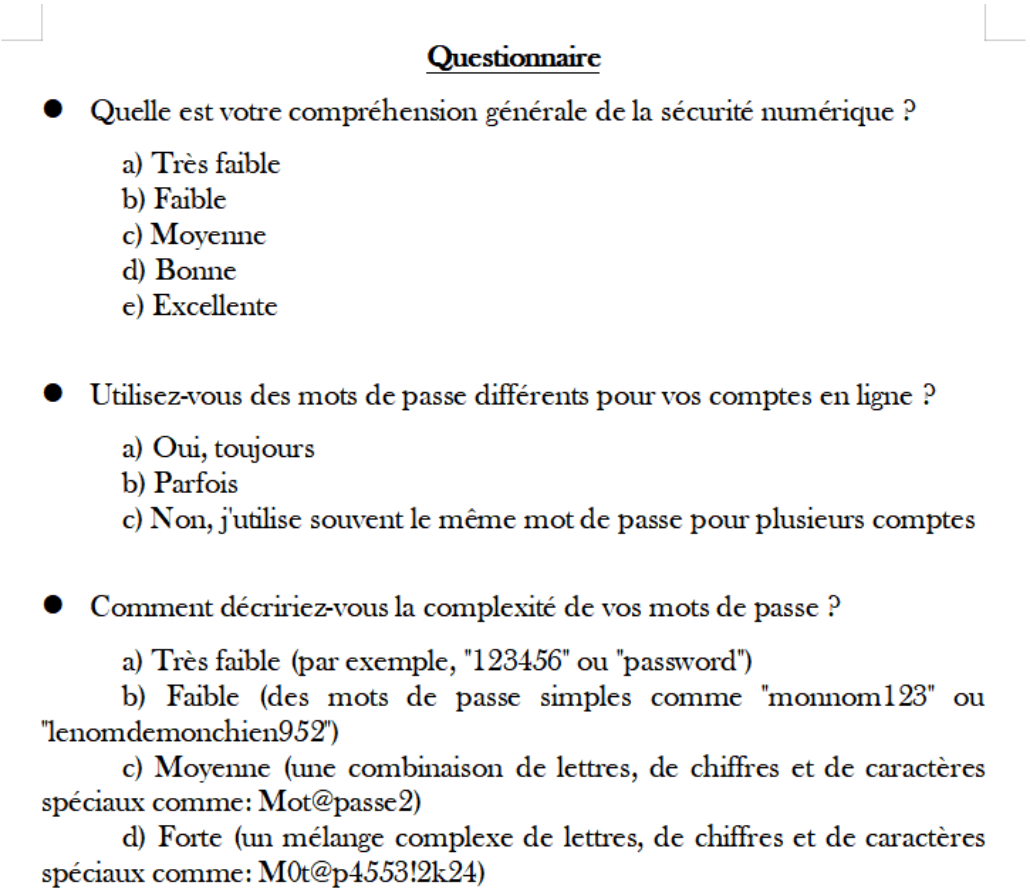
Conclusion Générale

La mise en place de campagnes de sensibilisation à la sécurité numérique à travers un Learning Management System (LMS) tel que Moodle s'est avérée être une bonne démarche pour renforcer la sécurité des utilisateurs du Ministère du Cadre de Vie et des Transports (MCVT). Les résultats positifs obtenus montrent l'impact significatif de cette initiative sur la conscientisation des utilisateurs quant aux enjeux liés à la sécurité numérique.

Ce travail met en lumière l'importance cruciale de l'éducation continue dans le domaine de la sécurité numérique, soulignant que la prévention à travers la sensibilisation fait partie des éléments clés pour faire face aux menaces croissantes. Les campagnes mises en œuvre ont réussi à faire faire un pas aux utilisateurs vers ce qu'ils doivent être : des acteurs informés et responsables, contribuant ainsi à réduire les risques potentiels liés à la cybercriminalité. Enfin, les résultats positifs encouragent à envisager la pérennisation de telles initiatives et à les adapter en fonction de l'évolution constante des menaces numériques. La sensibilisation à la sécurité numérique doit demeurer une priorité au sein de toute structure en général et au MCVT en particulier.

Annexe

Les Figures 3.9 à 3.11 montrent les questions composant le questionnaire soumis aux utilisateurs.



Questionnaire

- Quelle est votre compréhension générale de la sécurité numérique ?

  a) Très faible
  b) Faible
  c) Moyenne
  d) Bonne
  e) Excellente

- Utilisez-vous des mots de passe différents pour vos comptes en ligne ?

  a) Oui, toujours
  b) Parfois
  c) Non, j'utilise souvent le même mot de passe pour plusieurs comptes

- Comment décririez-vous la complexité de vos mots de passe ?

  a) Très faible (par exemple, "123456" ou "password")
  b) Faible (des mots de passe simples comme "monnom123" ou "lenomdemonchien952")
  c) Moyenne (une combinaison de lettres, de chiffres et de caractères spéciaux comme: Mot@passe2)
  d) Forte (un mélange complexe de lettres, de chiffres et de caractères spéciaux comme: M0t@p4553!2k24)

FIGURE 3.9 : Questionnaire (1/3)

- Utilisez-vous un gestionnaire de mots de passe pour gérer vos identifiants en ligne ?
  a) Oui
  b) Non
  c) Je ne sais pas ce que c'est

- Avez-vous déjà reçu des messages ou appels suspects prétendant être d'organismes officiels (comme l'administration fiscale) demandant des informations personnelles ?
  a) Oui, j'ai déjà reçu de tels messages
  b) Non, je n'ai pas reçu de telles sollicitations

- Êtes-vous méfiant vis-à-vis des liens et des pièces jointes provenant de sources inconnues ?
  a) Oui, je fais toujours preuve de prudence
  b) Parfois, cela dépend du contexte
  c) Non, je clique sans me poser de questions

FIGURE 3.10 : Questionnaire (2/3)

- Savez-vous comment vérifier l'authenticité d'un site Web avant de fournir des informations sensibles ?
  a) Oui, je vérifie toujours la légitimité du site
  b) Parfois, je le fais
  c) Non, je ne sais pas comment faire

- Connaissez-vous les risques associés au téléchargement de fichiers ou de logiciels piratés ?
  a) Oui, je sais qu'il y a des risques
  b) Je préfère ne pas le faire, mais je ne connais pas les risques précis
  c) Non, je ne suis pas conscient des risques

- Êtes-vous conscient des risques liés au partage d'informations personnelles sur les réseaux sociaux ?
  a) Oui, je fais attention à ce que je partage
  b) Parfois, je partage sans y penser
  c) Non, je partage tout ce que je veux

- Pensez-vous qu'il serait utile de faire de la sensibilisation à la sécurité informatique à l'endroit des utilisateurs du Ministère?
  a) Oui, ce sera utile
  b) Je ne sais pas vraiment
  c) Non, ce n'est pas utile

FIGURE 3.11 : Questionnaire (3/3)

Les programmes de sensibilisation mis en place sont illustrés par les Figures 3.12 et 3.13.

Thématiques	Sous-sections
I. Introduction au programme de sensibilisation et à la sécurité numérique	1. Importance de la sécurité numérique dans le monde professionnel 2. Présentation du programme et de ses objectifs
II. Gestion des mots de passe et authentification	➢ Création et pratiques de gestion des mots de passe forts.
III. Navigation Internet et Sécurité des E-mails	1. Navigation internet sécurisée ➢ Reconnaître les sites web sûrs. ➢ Utilisation sécurisée des réseaux Wi-fi publics. 2. Sécurité des e-mails et des pièces jointes ➢ Identifier les e-mails de phishing. ➢ Traiter les pièces jointes en toute sécurité. ➢ Règles de base pour les communications professionnelles par e-mail.

FIGURE 3.12 : Programme des campagnes de sensibilisation (1/2)

IV. Sécurité des Données et des Appareils	1. Protection des données ➢ Sensibilisation à la confidentialité des données. ➢ Sensibilisation sur le partage d'informations sur les réseaux sociaux. 2. Sécurité des appareils et des Logiciels ➢ Mises à jour système et logicielles. ➢ Antivirus: utilisation et mise à jour. ➢ Sécurité des appareils mobiles (smartphones, tablettes)

FIGURE 3.13 : Programme des campagnes de sensibilisation (2/2)

Les Figures 3.14 et 3.15 nous montrent respectivement les *Questions 1 et 4*

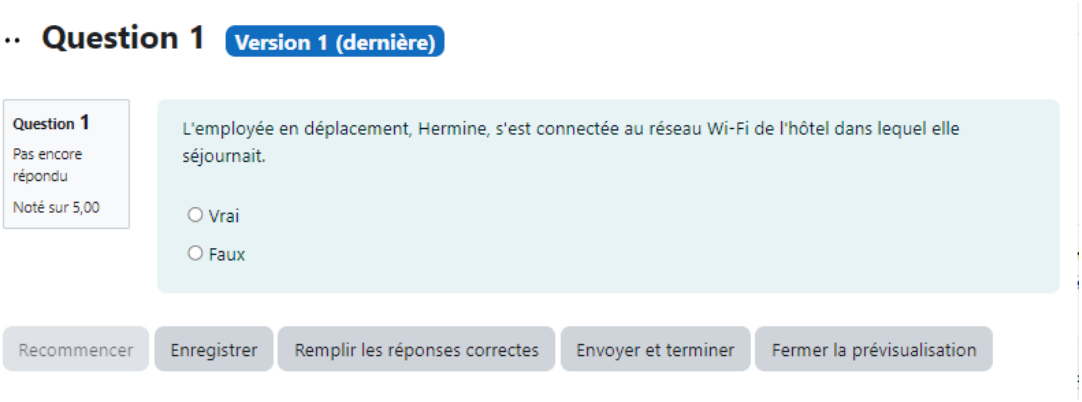


FIGURE 3.14 : Question 1 posée aux utilisateurs

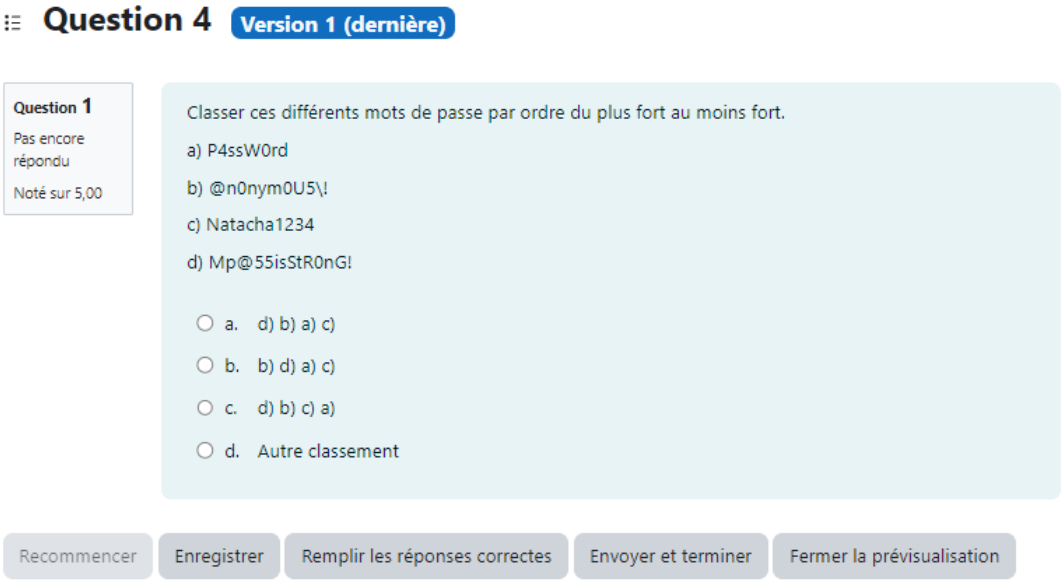


FIGURE 3.15 : Question 4 posée aux utilisateurs

Bibliographie

[1] Angus McIlwraith , *Information Security and Employee Behaviour*, Routledge, 2022.

[2] Ira Winkler, *Security Awareness For Dummies*, John Wiley & Sons, Inc, 2022.

[3] Bill Gardner & Valerie Thomas, *Building an Information Security Awareness Program Defending Against Social Engineering and Technical Threats*, Elsevier Inc, 2014.

[4] Mark Desman, *Building an Information Security Awareness Program*, AUERBACH PUBLICATIONS, 2002.

Webographie

[1] Sécurité numérique https://www.certitudenumerique.net/doc/memo/Memo_I-CERTitude_SecNUM.html, consulté le 06/01/2024.

[2] Les enjeux de la sécurité des systèmes d'information pour les entreprises et pour les individus https://www.carinel.com/post/les-enjeux-de-la-securite-des-systemes-d-information-pour-les-entreprises-et-pour-les-individus#:~:text=La%20protection%20des%20donn%C3%A9es%20sensibles%2C%20la%20continuit%C3%A9%20des%20op%C3%A9rations%2C%20la,compte%20pour%20minimiser%20les%20risques., consulté le 06/01/2024.

[3] Sensibilisation sécurité informatique : formez vos employés et protégez votre entreprise https://www.metacompliance.fr/blog-cybersecurite/sensibilisation-cybersecurite/pourquoi-la-sensibilisation-securite-informatique-est-importante, consulté le 06/01/2024.

[4] Qu'est-ce qu'un lms ? définition, explication et tout ce que vous avez besoin de savoir ! https://www.easy-lms.com/fr/base-connaissances/base-de-connaissances-lms/lms-cest-quoi/item10182, consulté le 06/01/2024.

[5] Installation de moodle https://docs.moodle.org/4x/fr/Installation_de_Moodle#Configuration_nÃl'cessaire, consulté le 07/01/2024.

[6] Moodle ubuntu : Install https://towios.vivaldi.net/moodle-ubuntu-install/, consulté le 28/12/2023.

[7] Méthodes d'échantillonnage : Types et exemples https://www.questionpro.com/blog/fr/types-dechantillonnage-pour-la-recherche-sociale/, consulté le 12/01/2024.

[8] Principe et utilisation de la loi de pareto (80/20) avec exemples https://www.manager-go.com/gestion-de-projet/dossiers-methodes/la-methode-des-20-80, consulté le 30/12/2023.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire ix

Introduction 2

1 Revue de Littérature 4

Introduction 4

1.1 Sécurité numérique 4

1.1.1 Qu'est ce que la sécurité numérique ? 4

1.1.2 Enjeux de la sécurité numérique 4

1.2 Sensibilisation à la sécurité numérique 5

1.3 Learning Management System (LMS) 5

1.3.1 Qu'est ce qu'un LMS ? 5

1.3.2 Avantages et Inconvénients à l'utilisation d'un LMS 5

Conclusion 6

2 Choix, installation du LMS et mise en place des campagnes de sensibilisation 7

Introduction 7

2.1 Choix du LMS 7

2.1.1 Critères retenus pour le choix du LMS 7

2.1.2 Etude comparative de quelques LMS 8

2.2 Mise en place de la plateforme LMS 9

2.3 Conception des campagnes de sensibilisation 13

2.3.1 Echantillonnage de la population constituant les utilisateurs 13

2.3.2 Analyse des besoins en matière de sécurité numérique des utilisateurs 13

2.3.3 Choix des thématiques des campagnes et mise au point du programme 14
2.3.4 Confection des modules de sensibilisation 14
2.3.5 Stratégie de promotion des campagnes auprès des utilisateurs 15
Conclusion 15

3 Résultats **16**
Introduction 16
3.1 Présentation de la plateforme 16
3.2 Analyse des indicateurs de performance 17
3.2.1 Le taux de participation 18
3.2.2 La compréhension des utilisateurs 18
3.2.3 Les changements de comportement 21
3.3 Perspectives 21
Conclusion 21

Conclusion **23**

Annexe **24**

Bibliographie **28**

Webographie **29**

Table des matières **30**