Challenge 48h

-Équipe 15-

DOCUMENT D'ARCHITECTURE TECHNIQUE

MOEUNG Siweil / ALBERT Nathalie / THOYER Gabby / GAMBIO Antonelly
RAVAN NABANLDIAN Orianne / JEANJEAN Alexis /NOEL Thomas

YNOV INFORMATIQUE | S.CELLYA

I.Contexte

Information Document :

Référence du document	Version	Date de diffusion	Département émetteur
Infrastructure/Dev/Cyber	1.0	13/04/2023	Ynov

Document délivré par :	
MOEUNG Siweil	B1 A Informatique
ALBERT Nathalie	B1 B Informatique
THOYER Gabby	B2 A Informatique
RAVAN NABANLDIAN Orianne	B3 Cybersécurité
JEANJEAN Alexis	B3 B Développement
NOEL Thomas	B3 B Développement
GAMPIO Antonelly	B3 Infrastructure

Suivi des modifications :

Version	Date	Objet
1.0	13/04/2023	Site web de prévention sur le phishing et cybercriminalité

Liste de destinataire :

Participant :	Poste :
MOEUNG Siweil	Dev Web
ALBERT Nathalie	Dev + Doc + Template
THOYER Gabby	Dev + Serveur + Template
RAVAN NABANLDIAN Orianne	Responsable de la documentation
JEANJEAN Alexis	Dev + Nav Bar + Template
NOEL Thomas	Dev + Arborescence + Template
GAMPIO Antonelly	Figma + Template

Introduction

Le phishing est une technique de cyberattaque qui consiste à tromper les utilisateurs pour obtenir des informations sensibles telles que des identifiants de connexion, des numéros de carte de crédit, etc.

Pour se protéger contre cette menace, il est important de sensibiliser les utilisateurs aux dangers du phishing et de leur apprendre comment éviter de tomber dans les pièges tendus par les fraudeurs.

Un site web de sensibilisation au phishing peut être un outil efficace pour aider les utilisateurs à comprendre les risques du phishing et à apprendre comment se protéger contre cette menace. Notre site web peut fournir des informations sur les types de phishing, les signes à surveiller, les erreurs à éviter et les mesures à prendre pour réduire les risques.

L'objectif principal d'un site web de sensibilisation au phishing est d'éduquer les utilisateurs sur les pratiques sécurisées en ligne et de les aider à reconnaître les tentatives de phishing. Il permettra de réduire les risques de vol de données sensibles et de protéger les utilisateurs contre les attaques de phishing.

Pour se faire nous avons décidé de créer un mail de phishing, l’envoyer à tous les étudiant d’Ynov et toutes les personnes qui cliquerons dessus seront automatiquement renvoyé vers notre site.

Cahier des charges détaillé

Objectifs :

Le site web de prévention sur le phishing et différents thèmes de cybersécurité doit :

- Sensibiliser les utilisateurs aux risques liés au phishing et à d'autres menaces de sécurité en ligne.
- Fournir des informations sur les meilleures pratiques de sécurité en ligne pour aider les utilisateurs à se protéger contre les attaques de phishing et autres menaces de sécurité en ligne.
- Proposer des outils, des astuces et des ressources pour aider les utilisateurs à identifier et à éviter les menaces de sécurité en ligne.

Fonctionnalités :

Le site web doit inclure les fonctionnalités suivantes :

- Pages d'accueil, à propos et ressources.
- Une section dédiée aux ressources, y compris des liens vers des sites tiers proposant des vidéos et des astuces pour aider les utilisateurs à se protéger contre les menaces de sécurité en ligne.

Design :

Le site web doit avoir un design moderne, professionnel et convivial pour les utilisateurs. Il doit être facile à naviguer et à utiliser, avec des sections claires et bien structurées. Il doit également être responsive, c'est-à-dire qu'il doit s'adapter à tous les types d'écrans, y compris les smartphones et les tablettes.

Contenu :

Le site web doit fournir un contenu informatif, utile et accessible pour les utilisateurs. Il doit être rédigé dans un langage clair et simple, afin d'être compréhensible pour tous les publics. Le contenu doit également être régulièrement mis à jour pour refléter les dernières tendances et menaces en matière de cybersécurité.

Hébergement :

Le site web doit être hébergé sur un serveur fiable, rapide et sécurisé pour assurer une disponibilité maximale et une performance optimale. Le choix de l'hébergeur doit être basé sur des critères tels que la fiabilité, la sécurité, la vitesse et le coût (0€).

Développement :

- Le site web doit être développé avec des technologies simple et fiable pour garantir une performance optimale dans le temps impartis. Les développeurs doivent utiliser des pratiques de codage sûres pour garantir la qualité du code.
- Des exemples concrets de tentatives de phishing et de fraudes en ligne pour sensibiliser les utilisateurs aux risques liés à la sécurité en ligne.
- Des ressources éducatives pour les enfants et les adolescents, y compris des conseils sur la façon d'utiliser les réseaux sociaux en toute sécurité et des astuces pour éviter les cyberprédateurs.

Questions Techniques

Présenter votre projet de façon la plus détaillée possible

Le projet que nous avons développé dans le cadre du challenge 48H répond à une problématique actuelle et importante pour les étudiants : la sécurité numérique.
En effet, la digitalisation de notre quotidien entraîne des risques qui peuvent coûter cher en termes d'argent et de sécurité. En créant un site de prévention pour les étudiants, Nous avons décidé d'aider à sensibiliser les étudiants aux risques liés à l'utilisation d'Internet, des réseaux sociaux et des ordinateurs.
En proposant 8 thématiques différentes : Phishing, Password, Stockage, Achat en ligne, Réseaux Sociaux, Téléchargement Logiciels, Connexion sur un Ordi Public, Utilisation Wifi Publique,

Nous avons pris soin de couvrir un large éventail de danger potentiels sur Internet, tels que la perte de données, le vol d'identité, l'usurpation d'identité, le piratage de comptes et les arnaques. En présentant ces sujets de manière simple et accessible, vous avez facilité la compréhension des étudiants, même ceux qui ne sont pas experts en informatique.

En fournissant des solutions simples et en sélectionnant des logiciels spécifiques pour aider les étudiants, vous avez apporté une réponse concrète aux problèmes rencontrés. Vous avez également créé un testeur de mot de passe pour aider les étudiants à évaluer la complexité de leurs mots de passe et à s'assurer qu'ils sont suffisamment sécurisés.

Nous avons choisi une approche pratique en envoyant un e-mail de phishing contenant un lien vers un site web que nous avons créé.

Notre site simule une attaque de phishing et permettra aux étudiants de comprendre les techniques utilisées par les cybercriminels pour voler des informations sensibles.

Nous croyons que cette méthode est efficace car elle permet aux étudiants de voir de manière concrète comment fonctionne une attaque de phishing et comment les cybercriminels utilisent l'ingénierie sociale pour tromper les victimes. Nous espérons que cette expérience aidera les étudiants à être plus prudents lorsqu'ils reçoivent des e-mails suspects et à mieux comprendre les risques liés à la cybersécurité.

Nous sommes convaincus que la sensibilisation à la sécurité informatique est essentielle de nos jours, car les cyberattaques sont de plus en plus fréquentes et sophistiquées. Nous espérons que notre projet aidera les étudiants à mieux comprendre les risques et à être mieux préparés pour se protéger contre les menaces en ligne.

Notre projet s'inscrit donc dans une démarche RSE en offrant une solution qui répond à un besoin social et environnemental, en l'occurrence la protection des données et la sécurité numérique. En sensibilisant les étudiants à ces enjeux, nous les aidons à devenir des citoyens responsables et à mieux appréhender les risques numériques dans leur vie quotidienne.

Présentez les différents cas d’usage que vous avez traités et justifiez leur priorisation.

La sensibilisation face aux dangers du numérique est aujourd'hui plus importante que jamais. Avec la digitalisation croissante de nos vies, il est essentiel que chacun prenne les mesures nécessaires pour protéger ses données et sa vie privée en ligne. C'est dans cette optique que notre projet a été conçu.

Nous avons choisi d'utiliser une méthode de sensibilisation originale : le phishing.

En effet, en envoyant un faux mail de phishing à une large audience, nous pouvons toucher un grand nombre de personnes et les forcer à s'informer sur les risques liés à ce type d'attaque. Notre but n'est pas de piéger les utilisateurs, mais de les alerter sur les signes à repérer pour ne pas tomber dans le piège d'un véritable mail de phishing.

Nous voulons que chaque utilisateur prenne conscience de l'importance de la vigilance en ligne. En les forçant à s'interroger sur les mails qu'ils reçoivent et sur les liens qu'ils cliquent, nous espérons que chacun sera plus attentif à la sécurité de ses données.

Nous avons également créé un site web avec 8 thématiques différentes pour aborder les différents aspects des dangers sur internet. Les informations sont présentées de manière simple et accessible pour que même les utilisateurs novices puissent comprendre.

Enfin, nous avons mis en place un testeur de mot de passe pour aider les utilisateurs à créer des mots de passe robustes et sécurisés. Un mot de passe complexe est l'une des premières barrières pour protéger ses données en ligne.

Notre projet est donc un outil précieux pour sensibiliser et éduquer les utilisateurs sur les dangers du numérique et leur apprendre à mieux se protéger. En prenant conscience des risques et en prenant les mesures nécessaires pour se protéger, chacun peut contribuer à rendre l'environnement numérique plus sûr et plus sécurisé.

En quoi votre projet s’imbrique dans la thématique du challenge ?

Notre projet s'inscrit parfaitement dans la thématique "améliorer la vie étudiante" du challenge.

En effet, la digitalisation de notre quotidien est une réalité qui touche tous les étudiants, et la sécurité numérique est un enjeu majeur dans ce domaine. En sensibilisant les étudiants aux risques liés à l'utilisation d'internet, nous leur offrons la possibilité de mieux protéger leurs données personnelles et financières, et donc d'améliorer leur vie étudiante en évitant des situations désagréables telles que le vol d'identité, le piratage de compte bancaire, etc.

De plus, notre projet est entièrement conçu par des étudiants pour des étudiants, ce qui renforce sa pertinence dans le cadre de ce challenge. Nous avons pris en compte les spécificités et les contraintes liées à la vie étudiante pour proposer une solution adaptée à leurs besoins et à leur niveau de connaissance en matière de sécurité informatique.

En offrant une solution simple et accessible à tous, nous permettons aux étudiants de s'informer et de s'interroger sur les enjeux de la sécurité numérique, ce qui contribue à leur éducation citoyenne et à leur développement personnel, deux éléments clés pour une vie étudiante épanouissante.

En quoi votre projet a une valeur ajoutée sur le marché actuel ?

Notre projet décrit ci-dessus a une grande valeur ajoutée sur le marché actuel, car il répond à un besoin croissant de sensibilisation à la sécurité numérique. Avec l'essor des technologies numériques, les menaces telles que le phishing sont de plus en plus courantes et les utilisateurs doivent être conscients de ces menaces et savoir comment se protéger.

En utilisant un mail de phishing pour sensibiliser les utilisateurs aux dangers de ces attaques, ce projet crée une opportunité unique pour les utilisateurs de se remettre en question et de prendre des mesures pour protéger leurs informations personnelles en ligne. En forçant les utilisateurs à s'informer et à s'interroger, le projet encourage également une culture de sécurité en ligne qui peut avoir un impact positif sur la sécurité globale des utilisateurs.

En outre, l'apprentissage de la création d'un mot de passe robuste est une compétence importante dans la sécurité numérique. En fournissant aux utilisateurs les connaissances nécessaires pour créer des mots de passe forts, ce projet peut aider à réduire les risques de piratage et de vol d'identité en ligne.

En somme, ce projet peut avoir une grande valeur ajoutée sur le marché actuel en aidant les utilisateurs à se protéger contre les menaces numériques et en favorisant une culture de sécurité en ligne plus responsable.

Comment vous êtes-vous organisés au sein de votre équipe pour mener à bien le projet ?

Nous avons défini des rôles clairs : chaque membre de l'équipe doit avoir une tâche précise à accomplir pour contribuer a notre projet. Il est important de définir des rôles en fonction des compétences de chacun. En l'occurrence nous avons opté pour : 5 Développeurs web (HTML/CSS), 1 Responsable du contenu à mettre sur notre site, 1 Créatrice de maquette et design du site.

Ensuite nous avons géré la planification. Elle est essentielle pour le bon déroulement du projet. Nous avons élaboré un plan d'action en déterminant les tâches à accomplir, les délais et les ressources nécessaires.

Pour se faire une communication régulière a été installé pour que chaque membre de l'équipe soit au courant de l'avancement du projet.

Nous avons fait en sorte de créer une répartition équitable des tâches pour éviter la surcharge de travail pour certains membres de l'équipe. Chaque membre doit s'est vu attribuer des tâches en fonction de ses compétences.

Nous avons régulièrement fait des points sur l'avancement du projet pour s'assurer que les objectifs sont atteints dans les délais impartis.

Chaque membre du groupe doit valider le contenu du projet.

Comment justifiez-vous les choix technologiques qui ont été faits ?

En 48 heures, notre principal objectif était de produire un résultat rapide et efficace. Nous avons opté pour une solution en full HTML/CSS, sans backend, qui nous permettait de nous concentrer sur l'essentiel : sensibiliser les étudiants au phishing.

Pour améliorer l'efficacité de notre site web, nous avons décidé de l'héberger sur GitHub, ce qui nous a permis de bénéficier d'un hébergement gratuit et de faciliter le partage de notre travail avec les membres de notre groupe. Nous avons également travaillé sur la qualité de notre projet en créant une maquette du site web ainsi qu'un mail de phishing réaliste, afin de renforcer l'impact de notre message auprès des utilisateurs.

Nous avons donc fait des choix stratégiques pour optimiser notre temps et notre efficacité, tout en gardant à l'esprit l'importance de la qualité de notre travail pour atteindre notre objectif de sensibilisation.

Sans rentrer dans un dossier de communication complet, par quel biais serait-il intéressant de promouvoir votre application/site ?

Travailler le référencement naturel de votre site web est essentiel pour améliorer sa visibilité sur les moteurs de recherche. Il est important de réaliser un audit SEO pour identifier les améliorations à apporter sur le site, telles que l'optimisation du contenu, des balises méta, des titres, des URL, etc.

La publicité en ligne est une option intéressante pour promouvoir votre site web. On pourrait utiliser des plateformes publicitaires telles que Google Ads, Facebook Ads, LinkedIn Ads, etc. pour atteindre votre public cible en fonction de vos objectifs de campagne.

Les réseaux sociaux peuvent être utilisés pour promouvoir votre site web. Créez des comptes sur les réseaux sociaux pertinents pour cibler et partager du contenu intéressant et engageant qui renvoie vers votre site web.

Collaborer avec des influenceurs pertinents pour prévenir des dangers du numérique auprès de leur audience.

Comment votre solution s’inscrit-elle ou peut-elle s’inscrire dans une démarche RSE ?

Une solution peut être conçue de manière à réduire sa consommation d'énergie et sa production de CO2. Par exemple, en utilisant des serveurs hébergeur éco énergétiques, en optimisant les performances du site ou en encourageant l'utilisation de matériel recyclé.

Une solution doit être accessible à tous, quel que soit le genre, l'âge, le handicap ou l'origine des utilisateurs. Il est important de concevoir des interfaces utilisateur qui soient conviviales pour tous les utilisateurs. Par exemple nous avons décidé d’opter pour une écriture inclusive.

Avec 2 journées de développement supplémentaire, qu’auriez-vous choisi de développer comme features et pourquoi ?

Avec 2 journées de développement supplémentaire, il y a plusieurs fonctionnalités intéressantes que nous aurions pu développer pour améliorer notre site web de sensibilisation au phishing. Tout d'abord, nous aurions pu utiliser un Framework tel que Angular, React ou Vue pour faciliter le développement et la maintenance de notre site. Nous aurions pu expliquer cela aux membres du groupe pour qu'ils comprennent mieux les avantages de l'utilisation d'un Framework et comment cela aurait pu aider à améliorer notre site.

Ensuite, nous aurions pu créer des espaces publicitaires sur notre site pour encourager les entreprises à sensibiliser leurs employés au phishing et à la sécurité informatique. Ces espaces publicitaires auraient pu être utilisés pour promouvoir des produits ou des services liés à la cybersécurité.

Nous aurions également pu mettre en place un véritable système de backend pour notre site, avec une fonction de connexion pour les utilisateurs et un forum de prévention. Ce forum aurait pu permettre aux utilisateurs de partager leurs expériences et de poser des questions sur la sécurité informatique, tout en offrant une plateforme pour que des experts puissent fournir des conseils et des solutions.

Enfin, nous aurions pu ajouter d'autres fonctionnalités à notre site, comme des simulations de phishing, des quiz de sécurité informatique et des tutoriels pour aider les utilisateurs à mieux comprendre les risques liés au phishing et à la manière de se protéger efficacement. Ces fonctionnalités auraient pu améliorer l'expérience utilisateur et aider à sensibiliser un plus grand nombre de personnes à la sécurité informatique.

Quelles évolutions avez-vous envisagées dans une V2 du projet ?

Ajout de fonctionnalités de sécurité supplémentaires :

Il serait possible de mettre en place des fonctionnalités de sécurité avancées pour aider les utilisateurs à se protéger davantage contre les attaques de phishing et autres menaces en ligne. Par exemple, on pourrait envisager de mettre en place un système d'authentification à deux facteurs pour renforcer la sécurité des comptes utilisateurs. Écrire un script afin que le mail soit nominatif.

Amélioration de l'expérience utilisateur :

Il serait possible d'améliorer l'interface utilisateur pour la rendre plus intuitive et facile à utiliser. On pourrait par exemple ajouter des fonctionnalités de glisser-déposer pour faciliter la création de messages de phishing, ou encore ajouter des animations pour rendre l'interface plus dynamique.

Développement d'une version mobile :

Avec de plus en plus d'utilisateurs qui accèdent aux sites web depuis leur téléphone portable, il serait intéressant de développer une version mobile du site web de sensibilisation au phishing. Cette version devrait être optimisée pour les petits écrans et offrir une expérience utilisateur adaptée aux appareils mobiles.

Intégration d'un système de suivi des statistiques :

Pour mesurer l'efficacité du site web de sensibilisation au phishing, il serait possible d'intégrer un système de suivi des statistiques pour suivre le nombre de visiteurs, les taux de clics, etc. Cette fonctionnalité permettrait de mieux comprendre comment les utilisateurs interagissent avec le site web et d'ajuster la stratégie en conséquence.

Collaboration avec des partenaires :

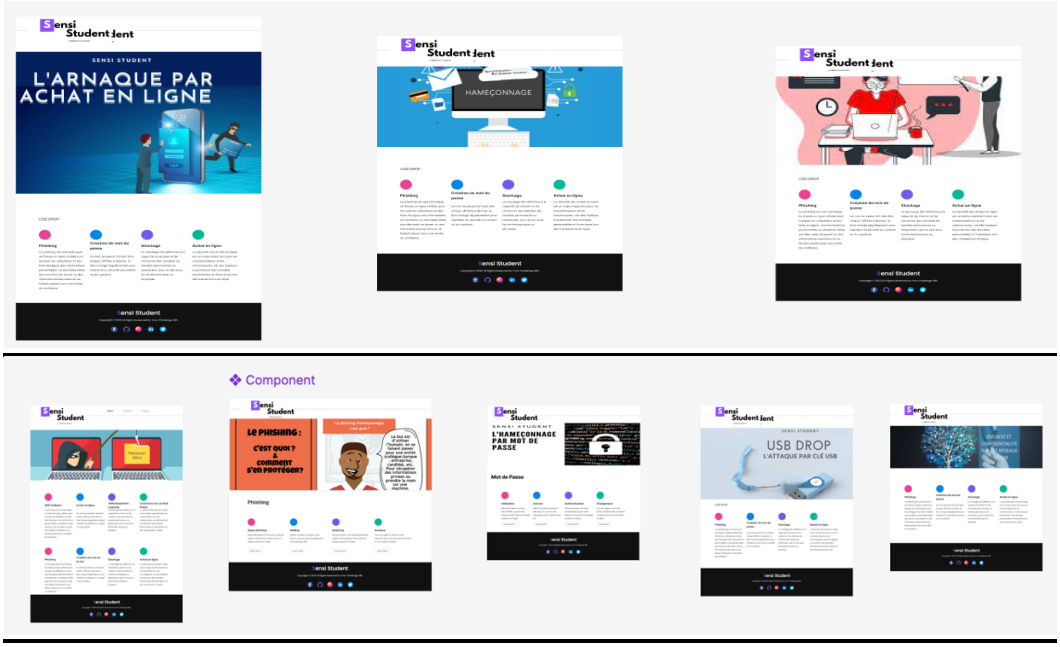
Pour toucher un public plus large et sensibiliser davantage de personnes aux dangers du phishing et de la cybersécurité, il serait possible de collaborer avec des partenaires tels que des écoles, des entreprises, des organisations gouvernementales, etc. pour diffuser le message de sensibilisation.

Annexe

Liens vers la vitrine : https://main--sparkling-madeleine-687c59.netlify.app

Liens vers notre site : https://calm-nasturtium-657d82.netlify.app

Maquette du site :



Maquette du mail de phishing :

Objet : Mise à jour du Compte Ynov

Chers étudiants,

Ce courriel est destiné à vous informer de la nécessité de mettre à jour votre compte Ynov pour l'une des raisons suivantes:

- Des informations inexactes ont été détectées dans votre profil.
- Mettez à jour votre adresse/numéro de téléphone actuels.
- Des détails supplémentaires sont requis pour compléter votre profil.

Cette mise à jour est obligatoire et nécessite une action dès la réception de ce courriel.

Pour continuer à utiliser votre compte Ynov, veuillez mettre à jour vos informations en cliquant sur le lien ci-dessous:

LE LIEN DE REDIRECTION (dans le style de l'annexe 1).

En l'absence d'action de votre part, nous serons dans l'obligation de suspendre votre compte de manière permanente.

Cordialement,

Faustin Édouard

+33 644629425

LYON ynov CAMPUS
Apprendre à réussir !