Kerberos Cybersécurité

Dossier de Campagne de Communication sur la Cybersécurité

Sommaire

Introduction

La cybersécurité est un enjeu majeur dans notre société connectée. Les cyberattaques, le vol de données et les escroqueries en ligne sont en constante augmentation, affectant à la fois les particuliers et les entreprises. Face à ces menaces, il est essentiel d'adopter de bonnes pratiques pour protéger ses informations personnelles et professionnelles.

Cette campagne de communication vise à sensibiliser le public aux dangers du numérique et à fournir des solutions concrètes pour se prémunir contre les cybermenaces. Pour ce faire, nous avons conçu une série de supports de communication incluant des affiches de sensibilisation et des publications sur Facebook, Instagram et LinkedIn, afin d'atteindre un large public de manière interactive et engageante.

Nous avons choisi une approche éducative et préventive, en mettant en avant des messages clairs et percutants pour encourager les bonnes pratiques en matière de cybersécurité.

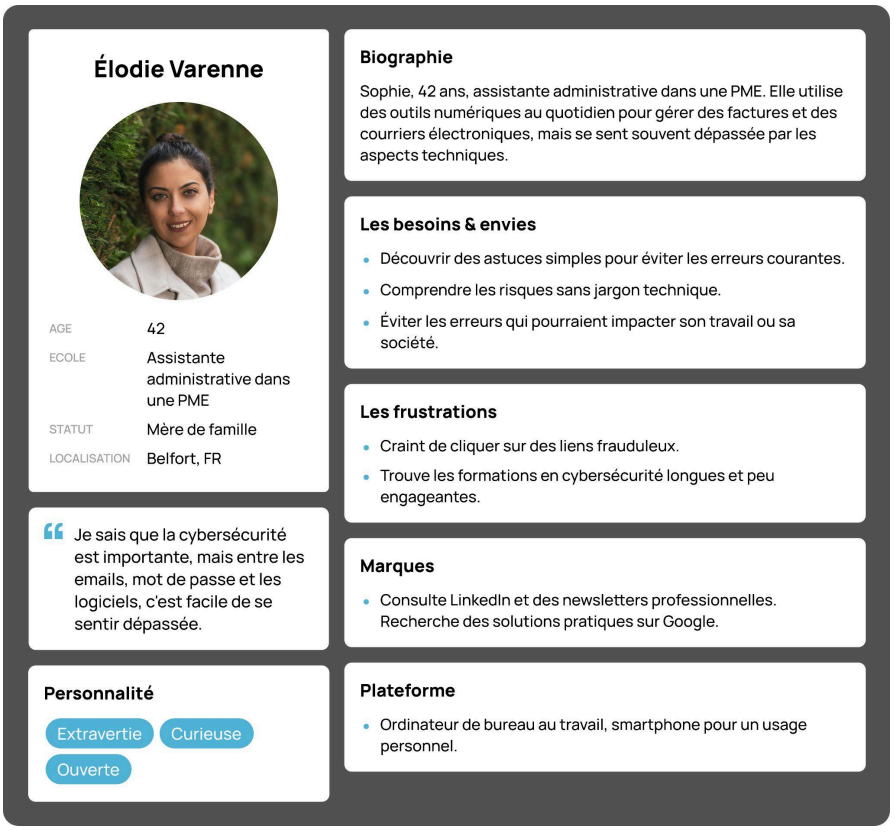
1. Objectifs de la campagne

Avec cette campagne, je vise plusieurs objectifs clés :

- **Informer** : Fournir des connaissances de base sur les cyberattaques courantes, comme le phishing et la gestion de mot de passe.
- **Éduquer** : Offrir des conseils pratiques et accessibles pour adopter des comportements sécurisés en ligne.
- **Prévenir** : Réduire le risque d'exposition aux menaces numériques en promouvant des outils et méthodes de protection efficaces.
- **Engager** : Encourager la participation du public via des interactions sur les réseaux sociaux et des défis ludiques liés à la cybersécurité.

2. Personas cibles

Pour m'assurer que cette campagne touche efficacement son public cible, j'ai analysé les profils les plus exposés aux menaces numériques et les plus susceptibles d'adopter des comportements à risque en ligne. J'ai identifié deux personas principaux qui reflètent des réalités différentes en matière d'usage du numérique, de niveau de sensibilisation et de besoin en cybersécurité.



Raphaël MALLET

AGE	21
ECOLE	Étudiant
STATUT	Seul
LOCALISATION	Montbéliard, FR

> "Je suis toujours en ligne, mais je n'ai jamais vraiment réfléchi à la manière de protéger mes données."

Personnalité

Extraverti | Joueur | Proche de sa famille

Biographie

Jules a 21 ans et est étudiant en gestion. Passionné par les réseaux sociaux et les jeux vidéo, il passe en moyenne 5 heures par jour sur les réseaux sociaux. Bien qu'il soit à l'aise avec les outils numériques, il n'est pas conscient de tout les risques de cybersécurité.

Les besoins & envies

- Apprendre de manière ludique et visuelle.
- Comprendre comment protéger ses données personnelles sans se compliquer la vie.

Les frustrations

- Trouve les interventions parlant de cybersécurité ennuyantes ou inutiles
- A peur de perdre l'accès à ses comptes en cas de piratage.

Habitudes de consommation

- Consomme beaucoup de contenu sur TikTok, Instagram et YouTube. Préfère les formats courts, divertissants et de vulgarisations.

Plateforme

- Smartphone principalement, ordinateur portable pour les études.

Ces deux personas permettent de mieux orienter le contenu de la campagne afin de proposer des formats et des messages adaptés à leurs besoins et comportements respectifs.

3. Supports de communication

3.1 Affiches de sensibilisation

J’ai conçu plusieurs affiches destinées à être diffusées dans des espaces publics, des écoles, des entreprises et sur les réseaux sociaux. Chaque affiche met en lumière un problème courant de cybersécurité accompagné d’une recommandation pratique.

Thématiques abordées :

1. Phishing et arnaques en ligne


ATTENTION AUX FAUX SMS DE LIVRAISON !
Ne tombez pas dans le piège des arnaques au colis
+33 6 89 XX XX XX
Nous avons essayé de livrer votre colis 00018357901, mais il n'y a aucun affranchissement. Suivez les instructions ici : kv88.us/AhvLS
Ne cliquez jamais sur un lien reçu par SMS sans vérifier directement sur le site officiel du transporteur.


CE SITE A L'AIR FIABLE... MAIS L'EST-IL VRAIMENT ?
Vous êtes sur le point d'entrer vos coordonnées bancaires... Êtes-vous sûr de ce site ?
paiement-bancaire.secure-xyz.com
Si un site vous paraît suspect, NE RENTREZ PAS vos informations bancaires !

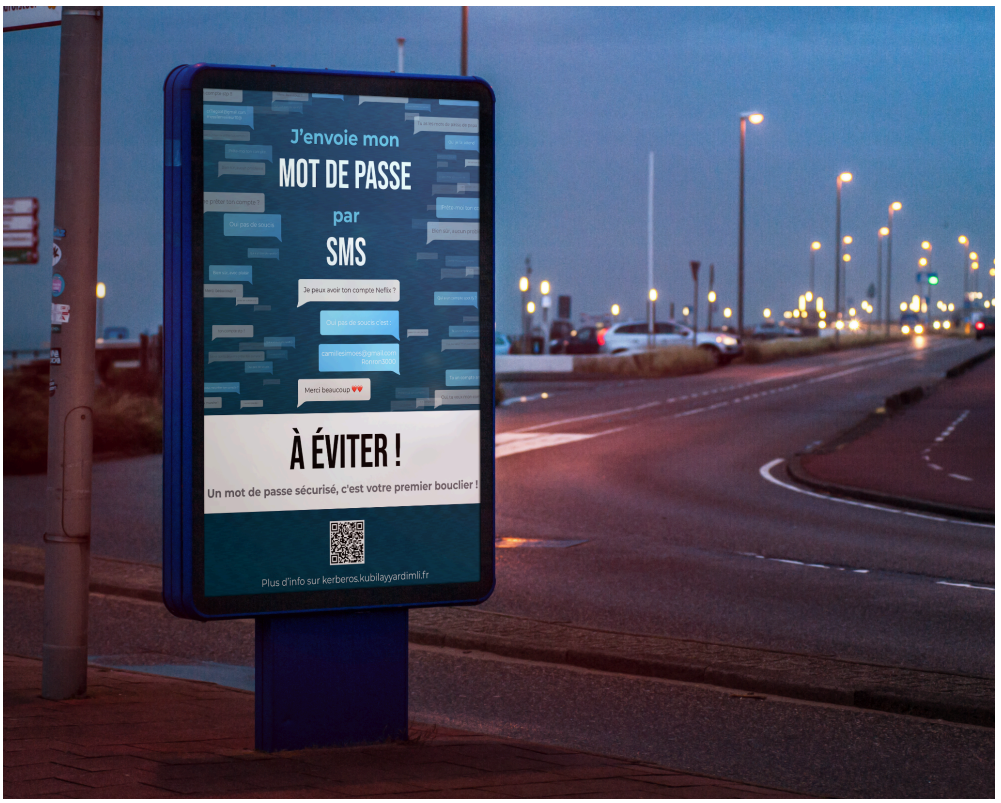
2. Gestion des mots de passe

Chaque affiche comprend un QR code dirigeant vers mon site officiel de la campagne (kerberos.kubilayyardimli.fr) pour approfondir le sujet avec des ressources supplémentaires.

3.2 Mockups des affiches de sensibilisation

1. Phishing et arnaques en ligne

2. Gestion des mots de passe


J'envoie mon
MOT DE PASSE
par
SMS
Je peux avoir ton compte Netflix ?
Oui pas de soucis c'est :
Merci beaucoup
À ÉVITER !
Un mot de passe sécurisé, c'est votre premier bouclier !
Plus d'info sur kerberos.kubilayyardimli.fr


connexxion
Je note mon
MOT DE PASSE
sur
UN POST-IT...
MAUVAISE IDÉE !
Un mot de passe sécurisé, c'est votre premier bouclier !
Plus d'info sur kerberos.kubilayyardimli.fr

3.3 Publications sur les réseaux sociaux

1. Facebook

KERBEROS Cybersécurité
October 11 ·

📦 Attention aux faux SMS de livraison ! 📦

Vous attendez un colis ? Un SMS vous demande de cliquer sur un lien pour payer des frais d'affranchissement ou vérifier votre adresse ? Méfiez-vous, c'est une arnaque ! 🚨

⚠️ Ne cliquez jamais sur ces liens !
⚠️ Ne partagez jamais vos informations personnelles !
⚠️ Vérifiez directement sur le site officiel du transporteur.

📌 La vigilance est votre meilleure protection contre le phishing !
👉 Plus d'infos sur : kerberos.kubilayyardimli.fr

#Cybersécurité #Phishing #SécuritéNumérique #FauxSMS #ProtectionDesDonnées

177 42 Comments 5 Shares

Like Comment Share

Most relevant

Write a comment...

View comments

2. Instagram

12,542 Likes

📱 Envoyer son mot de passe par SMS ? Mauvaise idée ! 🚫

Les mots de passe ne sont pas faits pour être partagés, et encore moins par message. Une fois envoyé, vous perdez tout contrôle dessus !

⚠️ Ne faites pas confiance aux messages privés pour échanger vos accès !
⚠️ Un mot de passe divulgué, c'est un compte en danger !
⚠️ Protégez vos comptes avec des mots de passe uniques et complexes.

🔐 Votre cybersécurité commence par de bons réflexes !
👉 Plus d'infos sur : kerberos.kubilayyardimli.fr

#Cybersécurité #MotDePasse #Phishing #SécuritéEnLigne #ProtectionDesDonnées

View all 123 comments

Add a comment... ❤️ 🙌

6 days ago

12,542 Likes

📩 Un email vous offre un cadeau ou un virement inattendu ? Attention au piège ! 🎣

Les hackers utilisent des emails frauduleux pour vous inciter à cliquer sur des liens malveillants. Une seule erreur et vos données personnelles sont en danger !

🚨 Astuces pour éviter le piège :

🔍 Vérifiez toujours l'adresse de l'expéditeur !
🔍 Ne cliquez jamais sur un lien douteux !
🔍 Ne téléchargez pas de pièces jointes suspectes !

🔐 Restez vigilant et protégez vos informations !
👉 Plus d'infos sur : kerberos.kubilayyardimli.fr

#CyberSécurité #Phishing #SécuritéEnLigne #EmailFrauduleux #ProtectionDesDonnées

View all 123 comments

Add a comment... ❤️ 🙌

3. Linkedin


KERBEROS CYBERSÉCURITÉ
350 Followers
8 hours •
Un mot de passe prévisible, c'est un compte en danger !
Trop de personnes utilisent encore des mots de passe évidents : prénoms, dates de naissance, ou autres informations personnelles facilement devinables.
Un mot de passe sécurisé doit être :
Long et complexe
Unique pour chaque service
Stocké de manière sécurisée
Ne facilitez pas la tâche aux hackers !
Investissez dans votre cybersécurité pour mieux protéger vos données.
Plus de conseils ici : kerberos.kubilayyardimli.fr
#Cybersécurité #SécuritéNumérique #ProtectionDesDonnées #MotsDePasse #HackingPrévention
MELISA08
JUSTINE08
HENRI2018
J'ai pris
LE PRÉNOM DE MON FILS
comme
ANGELO10
MOT DE PASSE...
ARTHUR12
YANNIS04
LUCAS2008
LOUIS2005
HUGO2016.
CAMILLE07
113
10 comments • 7 reposts
Like
Comment
Repost
Send

4.

KERBEROS CYBERSÉCURITÉ
350 Followers
8 hours •

🔍 Vous cliquez sur un lien sans vérifier l'adresse ? Mauvaise idée ! 🚨

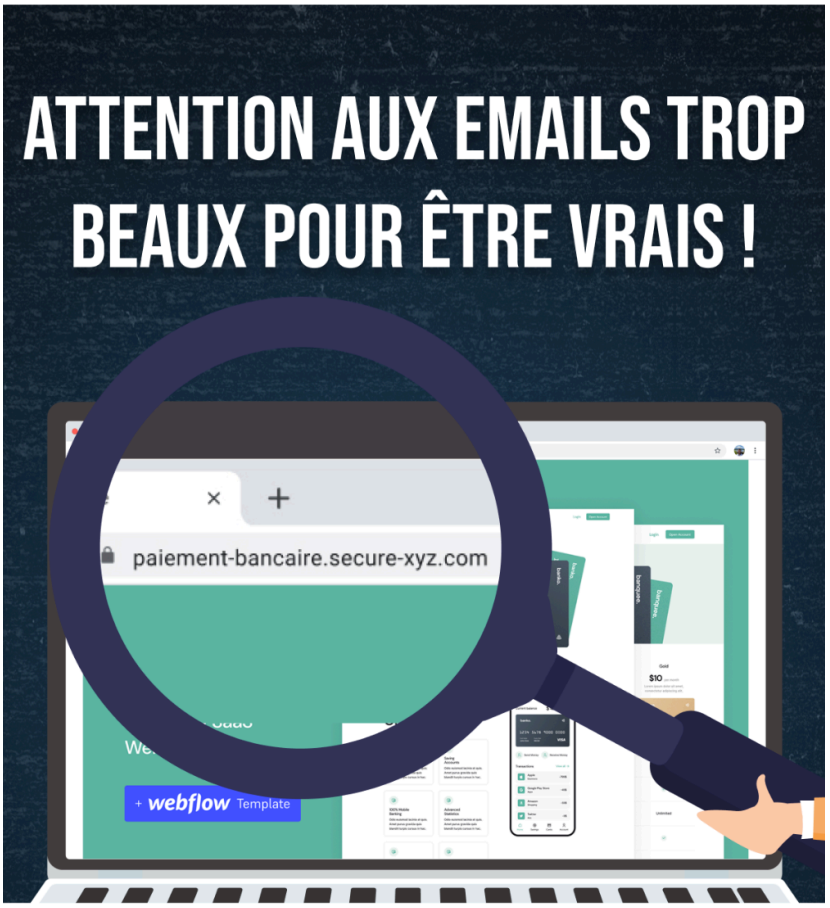
Les cybercriminels créent des sites web imitant parfaitement ceux des banques, des entreprises ou des services de livraison. Un simple clic peut compromettre vos informations sensibles.

💡 Comment repérer un lien frauduleux ?

✅ Vérifiez l'URL avant de cliquer
✅ Méfiez-vous des fautes d'orthographe dans l'adresse
✅ Ne renseignez jamais vos identifiants sur un site inconnu

📌 La cybersécurité est une affaire de vigilance et de bons réflexes !
👉 Plus d'infos sur : kerberos.kubilayyardimli.fr

#Cybersécurité #Phishing #ProtectionDesDonnées #SécuritéNumérique #FraudeEnLigne



113 10 comments • 7 reposts

Like Comment Repost Send

5.

4. Horaires de diffusion

Horaires de publication adaptés aux personas

Afin d'optimiser l'engagement, les horaires de publication ont été établis en fonction des habitudes de consommation de chaque persona :

Instagram

- **Lundi à 19h** : Carrousel détaillé sur une menace spécifique (heures de forte activité des jeunes adultes après les cours ou le travail).
- **Mercredi à 21h** : Story interactive (quiz, sondage ou questions ouvertes, idéal en soirée où l'engagement est fort sur Instagram).
- **Vendredi à 18h** : Infographie récapitulative (moment où les étudiants sont disponibles pour du contenu court et percutant avant leur sortie du week-end).

Facebook

- **Mardi à 12h** : Article détaillé avec explications et conseils sur un sujet de cybersécurité (adapté aux pauses déjeuner des actifs et étudiants).
- **Jeudi à 20h** : Vidéo explicative (format digestible après le travail et le dîner, moment idéal pour les professionnels qui consultent Facebook en soirée).
- **Samedi à 11h** : Infographie synthétique (format rapide et facile à consommer le matin avant les activités du week-end).

LinkedIn

- **Mardi à 8h30** : Post avec conseils de cybersécurité (publication avant le début de la journée de travail, moment clé sur LinkedIn).
- **Jeudi à 12h30** : Étude de cas sur une attaque de phishing (adapté aux pauses déjeuner des professionnels qui consultent LinkedIn pour s'informer).
- **Vendredi à 17h** : Infographie récapitulative sur les bonnes pratiques de cybersécurité (fin de journée, avant le week-end où l'attention est plus légère mais toujours informative).

5. Présentation du site et mises à jour

Le site kerberos.kubilayyardimli.fr est un élément central de cette campagne, offrant des ressources interactives et évolutives pour sensibiliser le public à la cybersécurité.

5.1 Pages principales

- **Gestion des mots de passe** : Cette page explique les bonnes pratiques pour sécuriser ses mots de passe, éviter les erreurs courantes et utiliser des outils comme les gestionnaires de mots de passe.
- **Phishing** : Cette page sensibilise aux différentes formes de phishing, montre comment repérer une tentative d'escroquerie et donne des conseils pour se protéger.
- **Jeux interactifs** : Une section dédiée aux jeux pour apprendre la cybersécurité de manière ludique. On y retrouve :
    - Un **Vrai ou Faux** sur la cybersécurité
    - Un **Quiz** pour tester ses connaissances
    - Un **Mots croisés** pour découvrir les termes clés de la cybersécurité

5.2 Mises à jour et évolution du site

Le site est conçu pour évoluer en fonction des nouvelles menaces et tendances en cybersécurité :

- **Mises à jour régulières** : Lorsqu'une nouvelle technique de phishing apparaît, la page dédiée sera mise à jour pour informer les utilisateurs.
- **Ajout de nouveaux jeux** : Si une nouvelle menace émerge, un jeu spécifique sera développé pour sensibiliser le public de manière interactive.
- **Amélioration continue** : Le site s'adapte en fonction des retours des utilisateurs et des évolutions technologiques pour offrir du contenu toujours pertinent.

Ainsi, cette plateforme reste un outil pédagogique évolutif, garantissant une sensibilisation continue aux enjeux de cybersécurité.

6. Conclusion et perspectives

J’ai conçu cette campagne pour offrir une approche accessible et engageante de la cybersécurité. En combinant affiches physiques, Facebook, Instagram et LinkedIn, ainsi qu’un site interactif mis à jour régulièrement, je maximise la portée de mon message tout en m’adaptant aux usages des différentes cibles.

À terme, cette initiative pourrait être enrichie par :

- Des collaborations avec des influenceurs pour élargir l’audience.
- L’ajout de nouveaux formats interactifs pour renforcer l’apprentissage.

L’enjeu est d’inscrire cette sensibilisation dans la durée, afin que chacun adopte des réflexes de cybersécurité au quotidien.

Kerberos Cybersécurité