LIVRE BLANC

10 astuces

Pour rendre le sujet de la cybersécurité plus accessible

par Amandine FULOP

Hello!

Moi c’est Amandine !

Jeune professionnelle actuellement en deuxième année de **mastère en expert stratégie digitale à l'ESD**. Depuis deux ans, j'ai l'opportunité d'effectuer une alternance chez **Phinasoft**, une start-up spécialisée dans le développement d'une solution d'**analyse et de gestion des risques cyber**. Au sein de Phinasoft, j'ai acquis une expérience concrète en tant qu'**UX/UI Designer et stratège digitale**. Mon rôle **polyvalent** me permet d'explorer divers aspects du monde numérique. Cette expérience me donne la possibilité de mettre en pratique mes connaissances théoriques et de développer une expertise dans des domaines tels que l'expérience utilisateur, la conception de site web ou le SEO, etc.

Mon intérêt pour la conception d'**interfaces intuitives et esthétiques** m'a conduit à me focaliser sur l'**ergonomie et l'accessibilité** des produits numériques que je crée. L'objectif est de les rendre conviviaux et faciles à utiliser pour un large public. Une attention particulière aux détails est primordiale, tout en cherchant des solutions créatives répondant aux besoins des utilisateurs. En parallèle de mes compétences en UX/UI Design, j'ai développé une solide compréhension des enjeux stratégiques du domaine digital. L'**analyse des besoins et des objectifs des clients** me permet d'élaborer des **stratégies pertinentes** et de mettre en place des **actions concrètes** pour atteindre les résultats souhaités.

La **curiosité intellectuelle** et la **rigueur** sont des atouts qui me permettent de rester constamment informée des dernières **tendances et innovations** en matière de stratégie digitale et d'expérience utilisateur. Cela me permet d'apporter **des solutions novatrices et adaptées à chaque projet** sur lequel je travaille.

Sommaire

Introduction

La cybersécurité est devenue une préoccupation majeure dans notre société hyperconnectée. Avec l'évolution constante des technologies, les risques liés à la sécurité en ligne sont de plus en plus présents et menaçants. Pourtant, malgré l'importance vitale de protéger nos informations personnelles et nos données sensibles, la cybersécurité reste souvent perçue comme complexe, technique et réservée aux experts. Cela crée une fracture numérique, laissant de nombreux utilisateurs vulnérables face aux cyberattaques.

Cybersécurité

Ce mot vous fait peur ?

Si je vous dis

> **La mise en œuvre d'une architecture de sécurité en couches avec des mécanismes de défense périmétriques contribue à atténuer les risques de compromission des systèmes d'information.**

Il vous faut un effort pour comprendre de quoi il s'agit avec ces termes techniques.

Alors que si je vous dis

> **L'utilisation de plusieurs niveaux de protection, aide à réduire les risques de piratage des systèmes informatiques.**

L'information est tout de suite beaucoup plus claire et accessible !

La cybersécurité est comme n'importe quel autre sujet, pour la rendre accessible à tous il faut adapter l'information à l'utilisateur, plus accessible, en créant des interfaces intuitives, engageantes et faciles à utiliser pour tous. **Heureusement, il y a quelques astuces utiles pour réussir cette mission !**
Vous voulez savoir lesquelles n'est ce pas ? Et si on faisait d'abord un point sur la cybersécurité.

01

Cybersécurité

Débutons par une définition du concept de cybersécurité et contextualisons son importance. À une époque où nos vies sont de plus en plus numérisées, où nous partageons une multitude d'informations sensibles en ligne, la sécurité numérique est devenue un enjeu critique. Ainsi, il est impératif comprendre pourquoi la cybersécurité plus accessible à tous devient un prérequis pour garantir la protection et la confidentialité de nos données dans ce monde interconnecté.

PRÉJUGÉ N°1

“Les hackers portent des capuches et travaillent dans des caves sombres. Ce sont tous des criminels malveillants.”

Alors qu'en est-il réellement ?

La vrai vie des hackers

Le saviez vous ?

Kristoffer von Hassel, né en 2008, est un jeune garçon américain reconnu comme **le plus jeune hacker** et chercheur en sécurité répertorié par Microsoft. À l'âge de cinq ans, il a **exposé des vulnérabilités dans le système Microsoft Live Xbox**, suscitant une large couverture médiatique en raison de son jeune âge.

Dans l'imaginaire collectif, les hackers ont souvent été représentés comme des individus sombres et malveillants, opérant depuis des caves obscures, vêtus de capuches. Cependant, **cette vision stéréotypée ne reflète pas la réalité complexe de ces acteurs numériques.** En examinant leurs profils variés, leurs motivations diverses, leurs compétences techniques et leur environnement de travail, il devient évident que **les hackers ne peuvent être réduits à ce simple cliché.**

Diversité des profils

Les hackers peuvent provenir de divers horizons et avoir des apparences et des environnements de travail classiques. ça peut être des professionnels de la sécurité informatique, des chercheurs en cybersécurité ou des hackers éthiques qui travaillent dans des bureaux.

Compétences techniques

Les hackers éthiques, les hackers en chapeau blanc cherchent à identifier et à corriger les vulnérabilités de sécurité, ainsi que les hackers en chapeau gris qui peuvent exploiter les vulnérabilités, mais sans intention malveillante. Il existe également des cybercriminels qui utilisent leurs compétences pour des activités illégales.

Motivations variées

Ils sont associés à des compétences techniques avancées en matière d'informatique et de sécurité. Celle-ci ne définissent pas forcément une intention criminelle. Nombreux hackers mettent à profit leurs connaissances pour protéger les systèmes et lutter contre les menaces cyber.

Les hackers ont des profils divers et joue un rôle central dans notre société numérique. Ils peuvent être motivés par des intentions bienveillantes, comme la sécurité informatique et l'éthique hacker, tout en reconnaissant qu'il existe également des individus malveillants. En démystifiant leur image et en comprenant leurs compétences et leurs environnements de travail, nous pourrons aborder de manière plus nuancée le monde complexe des hackers.

PRÉJUGÉ N°2

“Les programmes antivirus et les mots de passe complexes garantissent une sécurité totale.”

Alors qu'en est-il réellement ?

Les vulnérabilités informatique

Le saviez vous ?

En 2012, une société spécialisée dans la sécurité informatique a été engagée par le gouvernement du Royaume-Uni pour tester la sécurité de son réseau. Les experts en sécurité ont pénétré les défenses du gouvernement et accédé à un serveur contenant les mots de passe des utilisateurs. En examinant les mots de passe stockés, ils ont découvert que près de **1 000 employés utilisaient tous le même mot de passe pour accéder à leurs comptes : "Password123".**

Dans notre ère numérique en constante évolution, la question de la sécurité en ligne est primordiale. Cependant, l'idée répandue selon laquelle des mesures telles que des mots de passe complexes et des antivirus suffisent à garantir une protection totale est trompeuse.

La réalité est bien plus complexe, avec des facteurs humains, des vulnérabilités techniques et une innovation croissante des attaques qui remettent en question cette notion simpliste de sécurité absolue.

Evolution des attaques informatiques

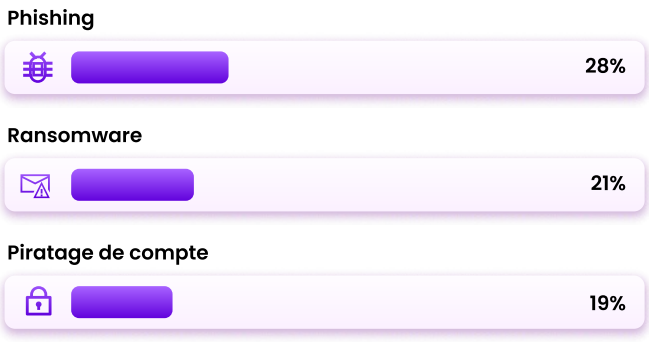
Les attaquants utilisent des techniques de plus en plus sophistiquées pour compromettre les comptes. Les attaques par force brute, le phishing, le vol de données, les attaques par dictionnaire, entre autres, sont des méthodes couramment utilisées. Même avec un mot de passe complexe, il existe des moyens pour les attaquants de contourner ou de compromettre la sécurité.

Failles humaines

Les utilisateurs peuvent commettre des erreurs susceptibles de compromettre la sécurité, même avec des mots de passe complexes. Par exemple, la réutilisation de mots de passe, la divulgation involontaire du mot de passe, la réponse à des attaques d'ingénierie sociale, etc. Les mots de passe complexes ne peuvent pas compenser les erreurs humaines ou la négligence.

Vulnérabilités techniques

Les vulnérabilités logicielles, les failles de sécurité et les erreurs de configuration peuvent exposer les mots de passe, peu importe leur complexité. Si un site ou un service est mal sécurisé et/ou que d'autres mesures de sécurité sont négligées, les mots de passe complexes et la sécurité du compte peuvent être compromis en raison de ces vulnérabilités techniques.



Les multiples vulnérabilités de natures et de typologies variées exigent une approche plus globale de la cybersécurité. **Une combinaison de mesures de sécurité, une éducation continue des utilisateurs et une vigilance constante sont nécessaires pour faire face aux défis croissants de la sécurité en ligne.**

On notera tout de même que 61 % des piratages sont dus à l'utilisation d'informations d'identification volées ou mal utilisées. ALORS ATTENTION A VOS MOTS DE PASSE !

PRÉJUGÉ N°3

“La cybersécurité est une tâche qui ne concerne que les informaticiens.”

Alors qu'en est-il réellement ?

Mieux vaut prévenir que guérir !

Le saviez vous ?

Selon le rapport d'enquête sur les compromissions de données publié par Verizon en 2023, 82% des compromissions impliquent le facteur humain (ingénierie sociale, erreurs, abus...).
Le télétravail et la multiplication des activités en ligne dans un contexte pandémique ont largement contribué à la croissance des attaques des applications web.

La cybersécurité ne concerne pas uniquement les informaticiens, mais elle est une responsabilité collective qui implique l'engagement de chacun. En effet, dans notre société de plus en plus connectée, nous sommes tous exposés aux risques liés à la sécurité numérique, que nous soyons des utilisateurs ordinaires, des entreprises, ou même des gouvernements. **Il est donc essentiel de comprendre que la cybersécurité est une préoccupation qui concerne l'ensemble de la société.**

Responsabilité partagée

La cybersécurité concerne les différents acteurs. Les utilisateurs finaux, qu'ils soient des particuliers ou des employés d'entreprise, ont également un rôle essentiel à jouer dans la protection de leurs informations personnelles et professionnelles. La sensibilisation, l'adoption de bonnes pratiques de sécurité et la vigilance lors de l'utilisation des technologies sont des aspects importants de la cybersécurité qui concernent tout le monde.

Sensibilisation du public

La cybersécurité ne se limite pas à la protection des systèmes informatiques, mais aussi à la protection des individus contre les menaces en ligne. Il est important d'éduquer le grand public sur les risques de cybersécurité, les meilleures pratiques de sécurité et les comportements à risque à éviter. Cela inclut la protection des informations personnelles, la lutte contre le phishing, l'utilisation de mots de passe forts, etc.

Collaboration entre les parties prenantes

La cybersécurité nécessite une collaboration entre les informaticiens, les utilisateurs, les décideurs, les organismes de réglementation, les forces de l'ordre et d'autres parties prenantes. Il s'agit d'un effort collectif pour protéger les systèmes, les données et les individus contre les cybermenaces.

80 %

Des cyberattaques

surviennent à cause de facteur humains

En conclusion, la cybersécurité ne peut pas reposer uniquement sur les épaules des informaticiens. C'est une question qui engage chaque individu, chaque entreprise et chaque institution. En prenant conscience de cette responsabilité collective et en travaillant ensemble, nous pourrons renforcer notre sécurité numérique et faire face aux défis croissants de l'environnement en ligne. **La cybersécurité est une priorité partagée qui nécessite une action commune de tous les acteurs impliqués.**

La cybersécurité, c’est quoi ?

Commençons par une explication

Définition

La cybersécurité est l'ensemble des mesures prises pour protéger les systèmes et données sensibles contre les attaques en ligne.

Les cybercriminels ciblent les informations personnelles des clients, telles que les noms, les adresses et les numéros de sécurité sociale, pour les vendre sur le marché noir. Cela entraîne une perte de confiance des clients, des amendes réglementaires et des poursuites judiciaires. Cependant, les organisations qui adoptent une stratégie de cybersécurité complète, utilisant des pratiques avancées, l'intelligence artificielle et l'apprentissage automatique, peuvent mieux se défendre contre les cybermenaces et réduire les conséquences des atteintes à la protection des données.

Quelques objectifs de la cybersécurité

- Protéger les systèmes et les réseaux
- Garantir le secret des informations
- Prévenir les violations de données
- Répondre aux incidents de sécurité

Cyberattaques les plus répandues

L’hameçonnage ou phishing

L'hameçonnage c’est des mails frauduleux, semblant provenir d'entreprises légitimes, qui incitent les utilisateurs à divulguer des informations sensibles. Cette pratique a augmenté durant la pandémie et le télétravail.

Rançongiciels ou ransomware

Un ransomware est un logiciel malveillant qui verrouille des fichiers ou des systèmes, menaçant de les effacer ou de divulguer des données sensibles, à moins qu'une rançon ne soit payée.

Les menaces internes

Les menaces internes résultent des employés ou partenaires ayant accès aux systèmes et échappant à la détection des solutions de sécurité, focalisées sur les menaces externes.

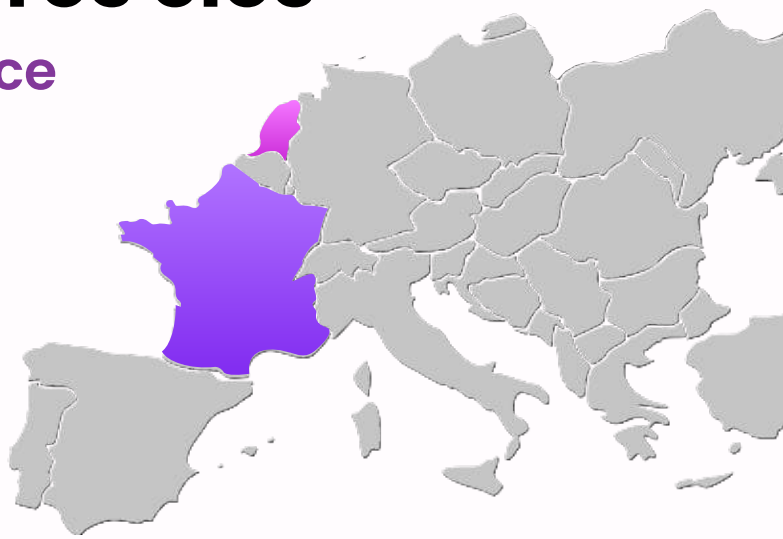
Il est essentiel d'être vigilant face aux cyber-menaces, en adoptant des pratiques de sécurité solides et en restant informé des dernières techniques utilisées par les attaquants afin de protéger nos données et notre vie privée en ligne.

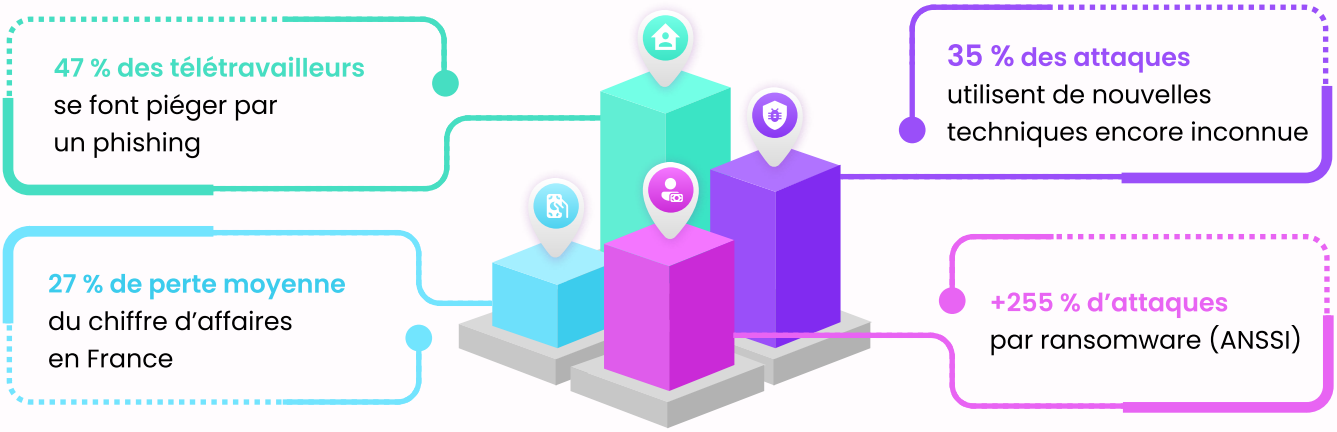
Contexte et chiffres clés

La cybersécurité en France

54 %
des entreprises
ont déclaré au moins une cyberattaque au cours de l'année passée.

2 ème
pays d'europe
Le plus touché par les attaques cyber après les Pays-Bas avec 57%.





Budget

Un investissement pour les entreprises

Bien que les attitudes en matière de protection des données évoluent, il reste encore beaucoup à faire. En 2022, on constate des changements dans les dépenses des entreprises, avec un budget plus conséquent pour la cybersécurité. Le budget alloué à la cybersécurité progresse, il représente à ce jour.

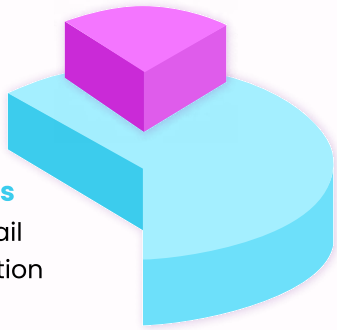
22% du total des dépenses informatiques.

Vulnérabilités

Les erreurs commises par les employés sont un point de préoccupation particulier.

28% des entreprises
ont sensibilisé plus de 75% de leurs employés aux risques

66% des organisations
estiment que le télétravail entraîne une augmentation des cybermenaces



Après une année 2022 qui a vu les cyberattaques s'accroître et le contexte mondial se tendre, la protection contre les cybermenaces devient un enjeu majeur pour les entreprises.

Chronologie des lois

Renforcement des défenses numériques pour une société résiliente

2004

Loi relative à la protection pénale de la propriété littéraire et artistique sur internet (HADOPI)
La protection des droits d'images, d'auteurs, chargée de lutter contre le téléchargement illégal en ligne.

2009

Loi pour la confiance dans l'économie numérique (LCEN)
Cette loi a introduit des dispositions relatives à la sécurité des réseaux et des systèmes d'information, ainsi qu'à la protection des données personnelles.

2011

Loi de programmation militaire (LPM)
Mesures renforçant la cyberdéfense, la protection des infrastructures vitales, le renforcement des capacités de surveillance et de réponse aux cyberattaques, en France.

2013

Stratégie nationale pour la sécurité des systèmes d'information (SNSI)
Renforcer la sécurité des systèmes d'information surtout la protection des infrastructures critiques et des administrations publiques.

2016

Loi de programmation militaire (LPM)
Renforcer davantage les capacités de cyberdéfense, établir un cadre de coopération entre les secteurs public et privé en matière de cybersécurité.

2018

Règlement général sur la protection des données (RGPD)
Règlement de l'Union européenne, pour renforcer la protection des données personnelles imposer aux organisations par le traitement des données.

2018

Loi pour une République numérique
Imposer des obligations de notification de violations de données et renforcer la responsabilité des prestataires de services en ligne.

2020

Schéma national de sécurité numérique (SNS)
Ce schéma a été élaboré pour renforcer la résilience des systèmes d'information et promouvoir une approche globale de la cybersécurité.

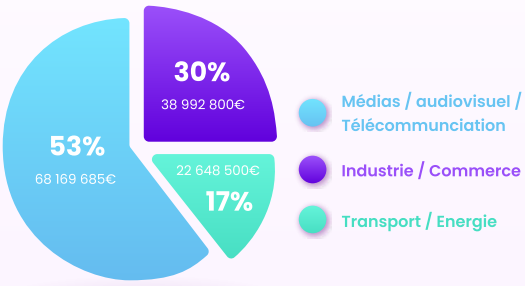
Le RGPD, c'est quoi ?

Une réglementation européenne

En pratique

Le règlement général de protection des données (RGPD) est un **texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne.** Il est entré en application le 25 mai 2018.
Le RGPD s'inscrit dans la continuité de la loi française « Informatique et Libertés » de 1978, modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles, établissant des **règles sur la collecte et l'utilisation des données sur le territoire français.**

Les secteurs les plus sanctionnés



Le RGPD s'adresse à toute structure privée ou publique établis sur le territoire de l'Union Européenne **effectuant de la collecte et/ou du traitement de données**, et ce quel que soit son secteur d'activité et sa taille.

Les missions du RGPD

Renforcer la protection des droits fondamentaux
Renforcer les droits des personnes concernant leurs données personnelles en leur donnant un meilleur contrôle sur leurs données personnelles.

Harmoniser la protection des données dans l'UE
Garantir un niveau élevé de protection des données personnelles dans le traitement des données à travers l'Europe, en favorisant la coopération.

Responsabiliser et promouvoir la conformité
Impose des obligations aux organisations qui traitent des données personnelles pour les responsabiliser et s'assurer qu'elles le font de manière légale et éthique.

Pourquoi le RGPD est aussi important ?

Le RGPD garanti la protection des droits fondamentaux des individus en matière de confidentialité et de contrôle de leurs données personnelles, dans un contexte de rapide évolution de l'environnement numérique. Les avancées continues dans les techniques de cyberattaques soulignent l'importance d'une réglementation solide pour contrer les nouvelles menaces pesant sur la sécurité des données. En fournissant un cadre réglementaire stricte, il incite les organisations à mettre en place des mesures de sécurité avancées et des stratégies de protection des données efficaces, leur permettant ainsi de faire face à ces défis en constante évolution.
Le RGPD joue ainsi un rôle essentiel en préservant la confidentialité des informations personnelles des individus et en renforçant leur confiance dans l'utilisation des services en ligne, dans un monde digital en perpétuelle innovation.

Les lois d'hier et de demain

La sécurité numérique en évolution constante

Loi Godfrain du 5 janvier 1988

Contrairement à ce qu'on pourrait s'imaginer, la législation autour de la sécurité informatique n'a pas commencé à se développer uniquement avec la transition digitale des entreprises. Les nouvelles technologies, en effet, font partie de la société et des préoccupations légales depuis bien avant. **La première loi française à cet effet est la loi Godfrain du 5 janvier 1988.**

Que réglemente la loi Godfrain en cybersécurité ?

Depuis sa promulgation, cette loi est un des fondements de la réglementation autour de la cybercriminalité et du piratage. Lorsqu'il est question du droit des nouvelles technologies de l'information et de la communication (NTIC), c'est donc cette loi qui s'applique. **Elle réglemente la falsification de documents informatisés, les systèmes de traitement ou toute tentative de délits informatiques en groupes organisés.**

Comment a évolué la loi Godfrain ?

Cette loi est impactée par trois textes, qui ajoutent quelques subtilités. Il y a d'abord la LCEN de 2004, qui ajoute une réprimande pénale lorsque des failles informatiques sont publiées ou fournies à des tiers. Ensuite, la directive 2009/136/CE qui implémente la nécessité d'alerter l'autorité compétente en cas de faille de sécurité. Enfin, le décret n°2012-436 du 30 mars 2012 qui applique la loi de 1978. Appelée "Loi Informatique et Libertés", elle réglemente le traitement des données et du fichage des individus.

Le cyberscore, ce sera quoi ?

Encourager les internautes à connaître les réalités des risques informatiques sur les sites qu'ils consultent fait partie des enjeux du gouvernement français. La loi du 3 mars 2022 y participe avec la création d'un cyberscore. Le visuel en question sera affiché sur les sites afin d'avertir l'internaute de la sécurité de celui-ci et des données hébergées. Pour obtenir ce score, les entreprises doivent réaliser des audits auprès de prestataires qualifiés par l'ANSSI.
Les critères et l'application du cyberscore seront précisés par arrêté d'ici son application au 1er octobre 2023.

On est tous concerné !

Les acteurs de la cybersécurité

La cybersécurité est devenue un enjeu majeur dans notre société interconnectée. Les avancées technologiques ont apporté de nombreux avantages, mais elles ont également ouvert la voie à de nouvelles menaces. La protection des données et la prévention des incidents de sécurité sont devenues des priorités pour tous les acteurs concernés. Les utilisateurs doivent mieux comprendre ces défis, pour mieux se préparer et adopter les mesures nécessaires pour renforcer sa sécurité en ligne.

Des professionnels aux particuliers

Les gouvernements

Ils gèrent des infrastructures essentielles, des données sensibles et des systèmes de communication critiques, qui peuvent être ciblés par des attaques de cybercriminalité. La cybersécurité est d'une importance vitale pour assurer la stabilité et la sécurité nationales.

Les entreprises

Elles sont confrontées à des défis de cybersécurité importants en raison de la valeur de leurs données sensibles et de leur rôle dans l'économie. Elles doivent prendre des mesures de sécurité pour protéger leurs informations, leurs systèmes internes et les données de leurs clients.

Les organisations à but non lucratif

Les organisations à but non lucratif travaillent sur des questions sensibles et collectent des données personnelles sur les individus. La protection de ces informations est cruciale pour maintenir la confiance de ces organisations.

Les utilisateurs individuels

Les particuliers sont exposés à diverses menaces en ligne, telles que le vol d'identité, le piratage de compte ou les logiciels malveillants. Ils doivent être conscients des risques et adopter des mesures de sécurité pour protéger leurs informations et leur vie privée.

La cybersécurité concerne absolument tout le monde, quelque que soit son âge son métier ou son niveau de maitrise de l'informatique. En rendant la cybersécurité accessible à tous, on enseigne les comportements responsables, on encourage une adoption plus large des bonnes pratiques et on renforce la sécurité face aux menaces en ligne.

L’importance chez les enfants

Un accès précoce à l’environnement numérique

A l'ère numérique actuelle, les enfants sont exposés très tôt aux technologies et à Internet, ce qui signifie qu'ils sont confrontés à des risques potentiels dès leur plus jeune âge. Par conséquent, les éduquer sur les aspects liés à la cybersécurité devient essentiel pour leur propre protection et pour développer des comportements en ligne responsables.

Pourquoi faut il former les plus jeunes ?

Naviguer en ligne en toute sécurité

Pour reconnaître les dangers tels que la divulgation d'informations personnelles, le cyberharcèlement, les prédateurs en ligne et les arnaques. En comprenant ces menaces et vulnérabilités, les enfants seront mieux équipés pour prendre des décisions éclairées et protéger leur vie privée en ligne.

Comprendre les risques et s’en protéger

Pour identifier les signes d'activités suspectes, comme les e-mails de phishing ou les logiciels malveillants, et adopter des mesures de prévention appropriées. Cela réduit les risques d'intrusion dans leurs systèmes, de vol d'identité ou de dommages causés par des logiciels malveillants.

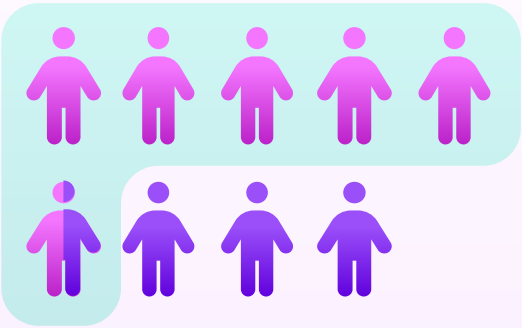
Promouvoir un comportement responsable en ligne

Pour apprendre les bases du respect des droits d'auteur, de la vie privée et de la manière de traiter les informations en ligne de manière éthique, pour favoriser la création d'une culture numérique positive et aider à prévenir les comportements nuisibles ou inappropriés.

Gérer l’identité numérique responsablement

Pour comprendre que tout ce qu'ils publient en ligne peut avoir des répercussions au long terme et qu'il est essentiel de construire une présence en ligne positive et sécurisé. Utiliser les paramètres de confidentialité et contrôler les informations qu'ils partagent, contribuent à protéger leur vie en ligne.

Et les parents, qu’en pensent-ils ?



9 parents sur 10 se disent dépassés par leurs enfants en termes de digital

78 %

d’entre eux pensent ne pas être assez informés sur la manière de protéger leurs enfants des dangers de l’informatique

60 %

déclarent ne pas se fier à leurs enfants quant à l’usage responsable des appareils et contenus digitaux.

La formation des enfants à la cybersécurité les habilite à naviguer en toute sécurité dans le monde numérique, à prendre des décisions éclairées et à protéger leur vie privée en ligne. Cela favorise la création d'une culture en ligne responsable et contribue à prévenir les risques liés à l'utilisation d'Internet et des technologies numériques.

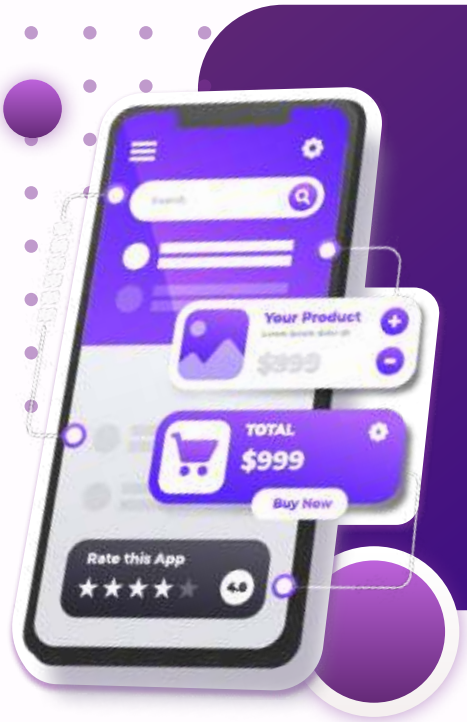
02

Astuces

La cybersécurité vous fait moins peur dorénavant ?
A présent vous comprenez les enjeux essentiels de la cybersécurité et l'importance de la rendre accessible à tous les utilisateurs et acteurs du digital. Voyons quelques conseils pour réussir cette mission et concevoir des interface et des expériences utilisateurs efficaces et abordable par tous.

UX Design

Créer une expérience fluide facile à prendre en main



L'UX, c'est quoi ?

L'UX ou expérience utilisateur, c'est la qualité globale de l'interaction qu'un utilisateur a avec un produit, un service ou un système. Les méthodes UX permettent de concevoir des expériences ergonomiques, qualitatives et simple d'utilisation pour les utilisateurs lorsqu'ils naviguent sur une interface, une application mobile, ou tout autre produit numérique.

Les utilisateurs sont au centre de la méthode UX, qui permet d'appréhender leurs besoins, attentes et comportements pour concevoir des interfaces intuitives, attractives et efficaces.

Les objectifs de l'UX

Simplicité
Créer des interfaces simples et intuitives

Adaptabilité
Adapter aux différents contextes d'utilisation

Engagement
Impliquer l'utilisateur dans son expérience

Pourquoi l'UX est un outil clé pour rendre la cybersécurité accessible à tous ?

Lorsque les produits de cybersécurité sont développés avec une méthodologie UX, cela signifie qu'ils sont conçus en tenant compte des besoins, des capacités et des préférences des utilisateurs. Cette approche centrée sur l'utilisateur permet de créer des interfaces et des expériences qui s'adaptent aux différents profils d'utilisateurs, rendant ainsi la cybersécurité plus accessible.

En comprenant les attentes, les connaissances et les habitudes des utilisateurs, les concepteurs UX peuvent créer des produits de cybersécurité qui sont faciles à utiliser et à comprendre, même pour les personnes non techniques.

Comment mettre en place une stratégie UX efficace ?

1

Comprendre les utilisateurs

Effectuez des recherches approfondies sur les utilisateurs cibles, leurs besoins, leurs motivations et leurs comportements. Utilisez des méthodes comme des enquêtes et des analyses de données pour obtenir des informations précieuses sur les attentes et les problèmes des utilisateurs.

2

Définir les objectifs

Identifiez clairement et efficacement les objectifs commerciaux et les objectifs d'expérience utilisateur que vous souhaitez atteindre grâce à l'étude menée sur votre cible. Ces objectifs doivent être alignés pour assurer une cohérence entre les résultats souhaités et les besoins des utilisateurs.

3

Concevoir des personas

Créez des personas représentant des archétypes d'utilisateurs afin de mieux comprendre leurs caractéristiques, leurs motivations, préférences et comportements. Les personas permettent de personnaliser l'expérience utilisateur en tenant compte des différents besoins et scénarios d'utilisation. Ils doivent être représentatif de la cible et établit à partir de l'enquête utilisateur.

4

Prototypage et test

Élaborez des prototypes interactifs de vos solutions UX, que ce soit sous forme de maquettes filaires, de prototypes fonctionnels ou de tests en situation réelle. Testez-les avec des utilisateurs pour évaluer leur convivialité, leur utilité et leur efficacité. Les résultats des tests permettent d'identifier les améliorations nécessaires avant le développement complet du produit ou du service.

5

Itération et amélioration continue

L'UX est un processus itératif. Utilisez les commentaires des utilisateurs et les données d'utilisation pour identifier les points faibles et apporter des améliorations constantes à l'expérience utilisateur. Effectuez des tests réguliers, mesurez les performances et adaptez votre stratégie UX en fonction des résultats obtenus.

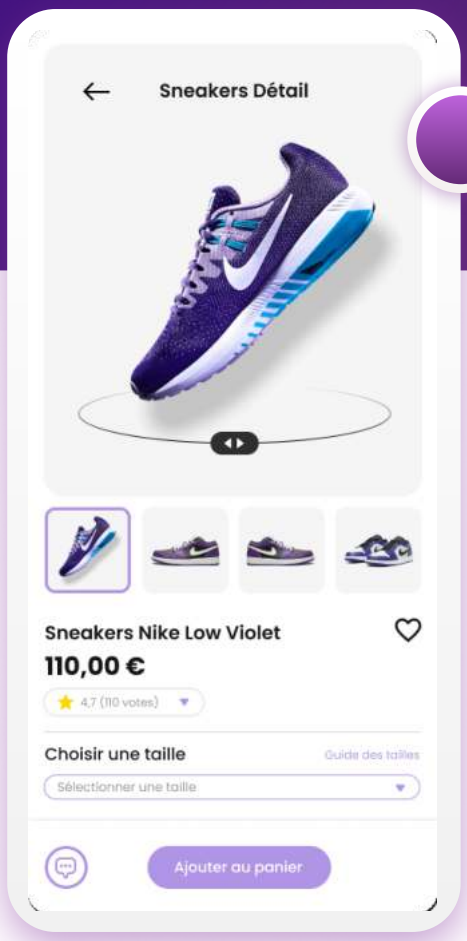
6

Collaboration multidisciplinaire

Impliquez une équipe multidisciplinaire dans la stratégie UX, comprenant des designers UX, des développeurs, des spécialistes du marketing et d'autres parties prenantes. La collaboration permet d'intégrer différentes perspectives et expertises, favorisant ainsi des décisions plus éclairées et une expérience utilisateur plus holistique.

UI Design

Créer une expérience attrayante visuellement



L'UI, c'est quoi ?

L'UI, ou Interface Utilisateur, est le moyen par lequel les utilisateurs interagissent avec un système informatique, une application ou un appareil électronique. Elle englobe tous les éléments visuels et interactifs. Une bonne conception d'UI met l'accent sur la clarté des informations présentées, la facilité de navigation, la cohérence des interactions, la réactivité aux actions des utilisateurs et l'esthétique globale de l'interface.
L'objectif principal de l'UI est de rendre l'expérience utilisateur aussi intuitive et efficace que possible, en permettant aux utilisateurs d'accomplir leurs tâches de manière fluide et sans confusion.

Les objectifs de l'UI Design

Clarté
Créer une interface organisée, une hiérarchie visuelle

Accessibilité
Considérer les limitations physiques et sensorielles

Ergonomie
Améliorer l'interaction des utilisateurs

Pourquoi l'UI Design est un outil clé pour rendre la cybersécurité accessible à tous ?

L'UI est un outil clé pour rendre la cybersécurité accessible à tous car elle joue un rôle crucial dans la communication entre les utilisateurs et les outils de sécurité informatique. En concevant une interface utilisateur claire et intuitive, on facilite la compréhension des mesures de sécurité et des actions à prendre pour se protéger en ligne.
Une UI bien conçue permet de présenter les informations de manière visuellement attrayante et organisée, de guider les utilisateurs, même ceux qui ne sont pas des experts en technologie, à travers les processus de sécurité afin de prendre des mesures de sécurité appropriées et de se protéger contre les menaces numériques

Une bonne interface utilisateur, c’est quoi ?

Les caractéristiques d’un UI Design efficace

Hiérarchie visuelle

L'interface doit utiliser une hiérarchie visuelle pour mettre en évidence les éléments importants et guider les utilisateurs. Utilisez des tailles, couleurs et espaces différenciés pour indiquer la relation entre les éléments.

Facilité de navigation

La navigation doit être simple et intuitive, permettant aux utilisateurs de naviguer facilement entre les différentes sections ou fonctionnalités de l’outil. Utilisez des menus clairs et une architecture d'information organisée.

Utilisation des couleurs

Les couleurs doivent être choisies avec soin pour attirer l'attention, indiquer les états ou les actions, et créer une ambiance visuelle agréable. Assurez-vous que les combinaisons de couleurs utilisées sont lisibles et accessibles.

Cohérence

L'interface doit suivre des conventions de conception cohérentes. Les éléments d'interface tels que les boutons, les menus et les icônes doivent être placés de manière prévisible et fonctionner de manière similaire dans tout le système.

Typographie lisible

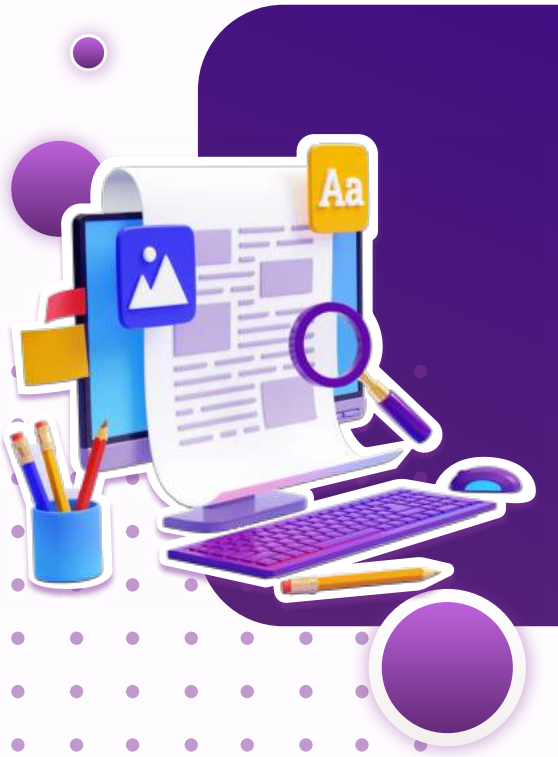
Choisissez une typographie adaptée à l'interface, avec des tailles de police lisibles et une bonne lisibilité. Utilisez des styles de texte différents pour mettre en évidence les informations importantes et faciliter la lecture.

Eléments interactifs

Les boutons, les liens et autres éléments interactifs doivent être facilement identifiables et réagir aux actions des utilisateurs de manière prévisible. Ils doivent être suffisamment grands pour être cliquables sur les écrans tactiles.

Langage accessible

Adapter la rédaction à la cible



Un langage adapté, c'est quoi ?

Un langage accessible répond de manière efficace et adaptée aux besoins des utilisateurs cibles, en tenant compte de leurs différents niveaux de connaissances et de compétences. Un langage clair, simple et compréhensible pour transmettre des informations de manière précise et pertinente à un public spécifique. Cela peut impliquer l'utilisation de termes techniques lorsque les utilisateurs ont le niveau requis pour les comprendre, tout en veillant à les expliquer de manière accessible pour les débutants.

Adapter le langage à la cible permet une communication claire et efficace. Chaque utilisateur assimile les informations de manière optimale, que ce soit en adaptant le niveau de complexité ou en fournissant des explications supplémentaires.

Les objectifs de la narration

Facilité
Simplifier le langage et les concepts

Accessibilité
Adapter l'information au niveau de l'utilisateur

Sensibilisation
Transmettre efficacement les informations

Pourquoi utiliser un langage adapté à la cible est un outil clé pour rendre la cybersécurité accessible à tous ?

La cybersécurité est un domaine en constante évolution, où la protection des données et des systèmes informatiques est d'une importance capitale. Cependant, la complexité inhérente à ce domaine peut souvent être un obstacle pour les personnes qui ne sont pas familières avec ses concepts et son vocabulaire technique. En utilisant un langage adapté, on peut expliquer les principes de base de la cybersécurité sans perdre les personnes en cours de route et démystifier ce domaine en apportant des informations de manière accessible et facilement assimilable.

L'utilisation d'un langage adapté peut contribuer à réduire l'écart de connaissances en matière de cybersécurité. En fournissant des ressources et des informations dans un langage accessible, on permet à un plus grand nombre de personnes de comprendre les enjeux liés à la sécurité en ligne et de prendre des mesures pour se protéger.

Comment adapter le langage à votre cible ?

Quelques conseils pour adapter le langage à votre cible

Simplifier les termes techniques

La cybersécurité est associée à un jargon technique complexe qui peut être déroutant pour les utilisateurs non initiés. Il est essentiel de simplifier les termes techniques en utilisant un langage clair et compréhensible pour le grand public. Évitez les acronymes et les termes spécialisés, ou expliquez-les de manière simple lorsqu'ils sont nécessaires.

Utiliser des termes concrets

L'utilisation d'exemples concrets peut aider les utilisateurs à comprendre les concepts de cybersécurité. Au lieu de se concentrer seulement sur les aspects techniques, illustrez les risques et les bonnes pratiques à l'aide d'exemples concrets et de scénarios réels auxquels les utilisateurs peuvent s'identifier. Cela rendra les informations plus tangibles et faciles à retenir.

Utiliser visuels et métaphores

Les visuels et les métaphores peuvent être des outils puissants pour expliquer des concepts complexes de manière visuelle et accessible. Utilisez des infographies, des schémas, des icônes et des illustrations pour accompagner le texte et faciliter la compréhension. Les métaphores peuvent aider à rendre des idées abstraites plus concrètes et faciles à assimiler.

Offrir des instructions

Décomposez les étapes en instructions claires et faciles à suivre. Hiérarchiser les actions à entreprendre et rendre les instructions plus digestes. Inclure des exemples concrets et souligner l'importance de suivre les étapes dans l'ordre, facilite la mise en pratique des mesures de sécurité et renforce la protection des données et des systèmes informatiques.

Découverte

Un cahier de vacances sur la sécurité informatique

Publié par l'association française ISSA France Security Tuesday en 2018, le cahier d'activités / de vacances « Les As du Web » vise à sensibiliser les enfants, à partir de 7 ans, sur le cyberespace. Il est disponible en ligne gratuitement sur le site : https://www.cybermalveillance.gouv.fr/medias/2019/11/ISSA_cahier_securite_numerique.pdf

> Ils doivent traiter les grands risques auxquels les enfants seront exposés de la manière la plus didactique et rassurante possible.
>
> **Gérôme Billois - Wavestone**

Storytelling

L’art de raconter pour éduquer

Le storytelling, c’est quoi ?

Le storytelling, ou l'art de raconter des histoires, est une technique de communication et de narration qui vise à transmettre un message de manière captivante et mémorable. Il consiste à utiliser des récits structurés pour engager le public et le plonger dans une expérience émotionnelle et immersive. Le storytelling repose sur l'idée que les êtres humains sont naturellement attirés par les histoires, qu'elles soient réelles ou fictives, et qu'elles ont le pouvoir de susciter l'empathie, de stimuler l'imagination et de favoriser la compréhension.

En utilisant le storytelling de manière stratégique, les entreprises, les organisations et les individus peuvent communiquer efficacement leurs idées, leurs valeurs, leurs produits ou leurs services, et créer des liens plus profonds avec leur public cible.

Les objectifs du storytelling

Compréhension
Rendre plus accessible des notions complexes

Sensibilisation
Raconter pour éduquer sur les risques et menaces

Changer les habitudes
Illustrer les bonnes pratiques pour encourager leur adoption

Pourquoi le storytelling est un outil clé pour rendre la cybersécurité accessible à tous ?

Le storytelling est un outil essentiel pour rendre la cybersécurité accessible à tous en simplifiant les concepts techniques complexes et en les contextualisant dans des histoires concrètes. La cybersécurité est un domaine qui implique de nombreux termes techniques et des menaces abstraites, ce qui peut rendre difficile sa compréhension pour les personnes non spécialisées. En utilisant des exemples concrets et des personnages auxquels le public peut s'identifier, le storytelling permet l'engagement émotionnel, facilitant ainsi la compréhension des enjeux de sécurité numérique.

En démystifiant la cybersécurité et en encourageant des comportements plus sécurisés, le storytelling sensibilise et éduque les gens, leur permettant ainsi de naviguer dans le monde numérique avec une plus grande autonomie et une conscience accrue des risques.

Comment mettre en place un storytelling efficace ?

1

Déterminer l'objectif

Identifiez clairement le message que vous souhaitez transmettre à votre public. Cela pourrait être l'importance de la sécurité en ligne, les risques liés à l'identité volée ou les conséquences d'une violation de données. Comprenez quel point clé vous voulez communiquer à travers votre histoire.

2

Créez des personnages

Développez des personnages auxquels votre public cible peut s'identifier. Donnez-leur des traits distinctifs, une histoire personnelle et des motivations. Les personnages peuvent représenter différents utilisateurs, tels qu'un étudiant, un parent, un employé ou un retraité, afin de toucher diverses perspectives.

3

Proposer des solutions

Intégrez des conseils pratiques et des mesures de sécurité dans votre histoire. Mettez l'accent sur les bonnes pratiques, telles que l'utilisation de mots de passe forts, la sensibilisation aux e-mails de phishing ou l'activation de l'authentification à deux facteurs.

4

Montrer les conséquences

Décrivez les conséquences réelles, illustrez les impacts émotionnels, financiers ou personnels que peuvent subir les personnages pour permettre aux utilisateurs de comprendre les risques et l'importance de prendre des mesures de sécurité appropriées.

5

Etablir un contexte

Définissez un cadre narratif réaliste pour votre histoire. Il peut s'agir d'une situation quotidienne, d'une expérience vécue ou d'un scénario spécifique lié à la cybersécurité. Assurez-vous que le contexte est pertinent et compréhensible pour votre public cible.

6

Conclure avec un message clé

Terminez votre histoire en réitérant le message clé que vous souhaitez transmettre. Résumez l'importance de la cybersécurité et encouragez les auditeurs à appliquer les enseignements tirés de l'histoire dans leur propre vie numérique.

Interactivité

Impliquer l'utilisateur

L'interactivité, c'est quoi ?

L'interactivité dans une expérience digitale, c'est la capacité des utilisateurs à participer activement et à influencer l'environnement numérique dans lequel ils interagissent. Cela implique une communication bidirectionnelle entre l'utilisateur et le système, permettant à l'utilisateur d'effectuer des actions, de prendre des décisions ou de fournir des informations qui sont ensuite traitées par le système pour générer une réponse ou un résultat. L'interactivité peut prendre différentes formes, telles que des boutons cliquables, des formulaires interactifs, du glisser-déposer, des simulations, des chats etc.

L'interactivité vise à créer une expérience plus engageante, personnalisée et immersive pour les utilisateurs, en leur permettant d'explorer et de contrôler activement le contenu et les fonctionnalités d'une plateforme ou d'une application numérique.

Les objectifs de l'interactivité

Engagement
Impliquer l'utilisateur dans l'expérience

Personnalisation
Adapter l'apprentissage au niveau des apprenants

Collaboration
Encourager le partage et la collaboration

Pourquoi l'interactivité est un outil clé pour rendre la cybersécurité accessible à tous ?

En permettant aux utilisateurs de s'engager activement, de pratiquer concrètement et d'adapter leur expérience d'apprentissage, l'interactivité favorise une meilleure compréhension et une rétention accrue des connaissances. Grâce à des outils interactifs, les utilisateurs peuvent acquérir des compétences pratiques en matière de gestion des risques et de protection de leurs données.

En suivant les progrès des utilisateurs et en évaluant leurs connaissances, l'interactivité permet également de fournir un retour personnalisé et de renforcer leurs compétences en matière de cybersécurité. En combinant ces aspects, l'interactivité joue un rôle clé pour créer une culture de la sécurité en ligne accessible à tous.

Comment créer une expérience interactive ?

Quelques mécaniques d’interactions mettre en place

Webinars interactifs

Organisez des webinaires interactifs où les participants peuvent poser des questions en direct, participer à des sondages et interagir avec les intervenants pour créer un environnement d'apprentissage interactif engageant et impliquant.

Scénarios et tutoriels interactifs

Développez des scénarios interactifs où les utilisateurs doivent prendre des décisions et faire des choix en matière de cybersécurité. Grâce à ces scénarios ils voient les conséquences de leurs actions ce qui renforce leur compréhension.

Simulateurs de situation réelles

Utilisez des simulateurs interactifs pour recréer des situations réelles de problèmes de sécurité. Les utilisateurs peuvent interagir avec ces simulations pour comprendre comment détecter et réagir face à des menaces spécifiques.

Plateforme de discussion

Créez des forums ou des plateformes de discussion interactives où les utilisateurs peuvent poser des questions, partager des expériences et échanger des conseils sur la cybersécurité. Cela favorise l'engagement et l'apprentissage collaboratif.

Environnements de sandbox

Mettez à disposition des environnements de sandbox où les utilisateurs peuvent expérimenter en toute sécurité différents aspects de la cybersécurité. Ils peuvent tester des outils de sécurité, simuler des attaques ou explorer des vulnérabilités sans risque pour leurs propres systèmes.

Sandbox (bac à sable)

Une sandbox, est un environnement isolé et contrôlé où les logiciels, les fichiers ou les processus suspects peuvent être exécutés en toute sécurité pour observer et analyser leur comportement sans risquer d'infecter ou de compromettre le système hôte.

Gamification

L’apprentissage par le jeu

La gamification, c’est quoi ?

La gamification est l'utilisation d'éléments et de mécanismes de jeu dans des contextes non ludiques afin d'engager, de motiver et d'influencer le comportement des individus. Elle consiste à intégrer des éléments de jeu, tels que des récompenses, des défis, des classements, des niveaux de progression et des interactions. La gamification est utilisée dans de nombreux domaines pour susciter l'intérêt et l'implication des individus.

L'objectif de la gamification est d'accroître l'engagement, la motivation et l'apprentissage en exploitant les instincts humains liés au jeu, comme le désir de réussir, la compétition, la curiosité et la satisfaction de gagner des récompenses.

Les objectifs de la gamification

Ludicité
Intégrer des mécaniques motivantes et divertissantes

Expérimentation
Permettre l’utilisateur de s’entrainer, de pratiquer

Assimilation
Rendre l’utilisateur acteur de son expérience

Pourquoi la gamification est un outil clé pour rendre la cybersécurité accessible à tous ?

La gamification est un outil essentiel pour rendre la cybersécurité accessible à tous en transformant l'apprentissage en une expérience ludique et engageante. En intégrant des éléments de jeu elle motive les utilisateurs à s'impliquer activement dans l'amélioration de leurs compétences en matière de sécurité. Elle permet un apprentissage pratique ce qui facilite la compréhension des bonnes pratiques de sécurité. En fournissant un suivi et une évaluation personnalisés, la gamification permet de mesurer les progrès individuels et de s'adapter aux besoins spécifiques de chaque utilisateur, contribuant ainsi à rendre la cybersécurité accessible et attrayante pour tous..

La gamification offre un moyen novateur et captivant d'aborder la cybersécurité, qui permet aux utilisateurs de s'impliquer activement dans le processus d'apprentissage et de développer leurs compétences en matière de cybersécurité de manière amusante et engageante.

Comment gamifier votre expérience digitale ?

Quelques mécanismes de jeu à intégrer

Identifier les objectifs

Déterminez les connaissances et compétences en cybersécurité que vous souhaitez enseigner à vos utilisateurs. Il est important de travailler sur chaque objectifs individuellement et de façon structurée pour offrir une expérience optimale à l'utilisateur et éviter la confusion.

Créer un système de récompense

Mettez en place un système de récompenses virtuelles pour encourager les utilisateurs à améliorer leurs connaissances et compétences en cybersécurité. Elles peuvent prendre la forme de badges, de niveaux, de points ou de récompenses spéciales.

Développer des défis interactifs

Concevez des défis de cybersécurité interactifs, comme des jeux, des énigmes ou des simulations, qui permettent aux utilisateurs d'appliquer leurs connaissances et de résoudre des problèmes de sécurité. Assurez-vous que les défis soient adaptés aux différents niveaux de compétence et progressivement plus difficiles.

Encourager la collaboration

Intégrez des éléments de collaboration, tels que des classements, des forums de discussion ou des défis d'équipe, pour encourager les utilisateurs à échanger leurs connaissances, à partager des conseils et à travailler ensemble pour résoudre des problèmes de sécurité.

Offrez des ressources pédagogiques

Fournissez des ressources éducatives, telles que des tutoriels, des articles informatifs et des vidéos explicatives, pour aider les utilisateurs à apprendre les bases de la cybersécurité et à comprendre les bonnes pratiques.

Suivre les progrès

Mettez en place un système de suivi des progrès des utilisateurs, leur permettant de voir leurs réalisations, leurs points gagnés et leur évolution dans le domaine de la cybersécurité. Cela les motivera à continuer à s'impliquer.

Découverte

Indata Jones - BNP Paribas

Dans un contexte de transformation Data, le Data Office de BNP Paribas Asset Management a fait appel à Brainsonic pour sensibiliser près de 3000 collaborateurs à l'univers de la Data et augmenter la qualité des données récoltées sur les différentes fonctions métiers.
https://www.cybermalveillance.gouv.fr/medias/2019/11/ISSA_cahier_securite_numerique.pdf

Interview de Hélène Batard . Head of Growth & Alexis Guittet . Head of cybersecurity

Hélène Batard .
Head of Growth

Je gère toute la partie croissance et plutôt marketing de la marque sur la partie notoriété acquisition et conversion.

Alexis Guittet .
Head of Cybersecurity

Je travaille aussi dans la stratégie cyber dans la boîte Seela et anciennement Product Manager de BattleHack.

On s'est rendu compte très rapidement qu'il nous fallait une plateforme dédiée pour le cyber entraînement. A partir de ce postulat, on a créé **BattleHack : La plateforme compétitive avec des challenges complexes et un environnement stimulant, pour parfaire vos compétences en cybersécurité offensive et défensive.**

Quelles sont les principales différences entre la formation de la cybersécurité via BattleHack et les méthodes classiques ?

Nous appelons ça le "Golden Bridge", l'objectif est d'établir un lien étroit entre la formation dispensée sur Seela et les missions effectuées sur BattleHack. En d'autres termes, chaque module de la formation sur les vulnérabilités est accompagné de missions correspondantes sur la plateforme de cyber-training. De plus, si vous rencontrez des difficultés lors d'une mission sur BattleHack, nous vous proposons également un cours de formation sur la cybersécurité. En résumé, nous nous assurons que les apprenants disposent en permanence d'exercices et de possibilités de réflexion, afin de garantir une expérience d'apprentissage complète et stimulante.

Comment la gamification a-t-elle été intégrée dans BattleHack pour rendre la cybersécurité plus accessible ?

La direction artistique dans l'industrie du jeu vidéo présente un intérêt particulier, car elle permet au joueur de comprendre rapidement les objectifs à atteindre, quel que soit le jeu. Lors de nos discussions avec les équipes de conception, nous avons convenu de créer une expérience ludique et stimulante. Dans un domaine comme la cybersécurité, qui est souvent perçu comme technique et peu visuel, l'introduction d'éléments de jeu offre un avantage graphique dynamique. La cybersécurité est souvent considérée comme statique, linéaire voire binaire, mais nous avons réussi à combiner ces deux mondes de manière harmonieuse pour proposer un produit à l'esthétique soignée.
Le monde de la cybersécurité est vaste, avec des spécialistes travaillant dans différents domaines tels que la sécurité offensive, la défense, le web, le management ou l'architecture, pour n'en nommer que quelques-uns. Notre objectif, à travers la direction artistique de BattleHack, est de définir des rôles en cybersécurité à travers nos personnages. La composition et la réflexion de ton équipe auront une influence directe sur votre progression.

Chaque personnage possède ses propres caractéristiques physiques qui reflètent leurs compétences respectives. Par exemple, Monsieur Musclor incarne la force brute. Nous avons vraiment accordé une grande importance à la création de personnages dont l'apparence est en adéquation avec leurs compétences, car cela constitue un élément clé de notre approche ludique.

Comment la gamification aide les utilisateurs à mieux comprendre les concepts de cybersécurité ?

Nous allons exploiter les biais cognitifs évidents pour notre public cible, à savoir les 18-35 ans. Dans les jeux vidéo et les applications d'aujourd'hui, il est courant de recevoir des récompenses virtuelles sous forme de points que l'on peut dépenser dans un magasin virtuel après avoir accompli une tâche. Nous avons naturellement intégré ce concept de gratification virtuelle dans BattleHack. Les joueurs et les apprenants utilisent notre plateforme comme un CV interactif. En réalité, à la fin de chaque mission, en fonction de leur performance, les participants accumulent un certain nombre de points. Ces points sont ensuite utilisés pour établir un classement général. Notre objectif est que, en jouant sur BattleHack, un recruteur puisse évaluer rapidement la valeur d'un candidat en se basant simplement sur le nombre de points qu'il a obtenu sur la plateforme. Parallèlement, nous sommes en train de développer un mode de jeu multijoueur. Dans ce mode, deux équipes s'affrontent et un classement distinct est établi en fonction du niveau de chaque équipe et de chaque participant. L'idée est de permettre aux joueurs de se mesurer à des équipes ou à des individus en fonction de leur niveau de compétence.
En résumé, notre approche combine habilement les principes de gratification virtuelle avec un système de classement qui permet aux utilisateurs de démontrer leurs compétences et de se positionner par rapport à d'autres joueurs et équipes.

Comment l'aspect compétitif de la plateforme motive les utilisateurs ?

L'ego Boost ! Un aspect clé de la compétition réside dans notre système de classement. Atteindre le rang numéro un et remporter le trophée donne le sentiment d'être le Boss, en maîtrisant chaque aspect du jeu. En parallèle, nous valorisons la notion de communauté, où l'échange de connaissances, de théories et d'outils est encouragé. Partager ces ressources crée un sentiment de bienveillance et de pédagogie et permet de laisser une empreinte positive sur notre canal Discord.

Nous cherchons à aller encore plus loin avec BattleHack, en mettant en place une connexion directe entre les joueurs les plus talentueux de notre plateforme et les entreprises. La compétition pour atteindre les sommets du classement vise également à attirer l'attention des recruteurs, qui cherchent activement les meilleurs candidats . Elle ouvre de nouvelles opportunités pour ces talents de se faire remarquer et de décrocher les meilleurs emplois possibles. Dans l'ensemble, notre approche allie compétition et collaboration, offrant aux joueurs la possibilité d'exceller tout en favorisant une atmosphère d'entraide conviviale.

Quelle était la cible de BattleHack lorsque vous avez commencé à le développer ?

À l'époque, la plateforme cyber-training comptait déjà plusieurs clients, chacun ayant des besoins et des attentes spécifiques. Le but était de renforcer les compétences internes en matière de cybersécurité, de protéger davantage l'entreprise et de convertir des profils vers des carrières en cybersécurité, où le recrutement est souvent difficile. Puis nous avons élargi notre champ d'action au secteur B to C, bien que cela ne soit pas notre public cible initial, dans le but de toucher un public plus large.

Au sein d'une équipe, il y a toujours une diversité de profils. De l'expert jusqu'à l'apprenti ou le stagiaire, les besoins peuvent varier considérablement. Nous sommes conscients de cette réalité et nous nous efforçons de répondre à chaque besoin spécifique.

Comment avez-vous valider la correspondance de BattleHack avec les besoins de votre cible ?

Tout d'abord, notre victoire lors du cyber Night a été une immense source de satisfaction. C'était extrêmement encourageant de voir que notre projet prenait forme et suscitait l'engouement. De plus, les retours positifs que nous recevons de certaines personnes par messages privés, qu'il s'agisse de leurs retours d'expérience ou de la remontée de bugs, sont également très gratifiants. Ces personnes reconnaissent le potentiel de notre plateforme, investissent du temps et souhaitent contribuer à son amélioration. Pour moi, l'échec se produit lorsque quelqu'un visite la plateforme, ne s'engage pas et ne revient jamais. Notre communauté continue également de grandir, avec un afflux d'utilisateurs sur notre serveur Discord. Il y a même deux ou trois joueurs qui se distinguent en tant que meilleurs et qui nous aident à répondre aux autres utilisateurs. La présence et l'investissement de ces joueurs de qualité sur notre plateforme sont un signe que nous sommes sur la bonne voie.

Pour moi, le véritable succès est lorsque nous recevons des témoignages de personnes qui découvrent notre plateforme et qui sont impressionnées par son design incroyable et la qualité des missions proposées. Notre design est une véritable force et nous permet de nous différencier. Nous souhaitons sortir des codes traditionnels du domaine de la cybersécurité, souvent brute, en offrant un effet "Waouh" à nos utilisateurs. Nous gamifions l'apprentissage tout en considérant les besoins des entreprises, en proposant une expérience éducative dynamique. Nous ciblons également les jeunes utilisateurs qui sont extrêmement exigeants en termes d'UX/UI et nous nous efforçons de ne pas les décevoir.

Comment BattleHack s'adaptent aux différents niveaux des utilisateurs ?

Les premières missions sont conçues dans le but de familiariser les utilisateurs avec les concepts fondamentaux de la cybersécurité. Quant aux dernières missions, elles sont spécifiquement conçues pour présenter des défis plus corsés et vous pousser à vous investir davantage. Notre objectif est de garantir que même les experts les plus chevronnés soient confrontés à des obstacles stimulants pour réussir les missions. La difficulté des missions réside dans le nombre d'étapes à franchir et leur complexité croissante.

Est-ce que vous avez fait des évolutions suite à des retours utilisateurs ?

Nous sommes en perpétuelle évolution et recherche d'amélioration. Nous sommes conscients que nos utilisateurs attendent de nous de l'innovation, tout en ayant la nécessité de résoudre les éventuels problèmes techniques, ce qui nous amène à gérer nos priorités de manière équilibrée.

Nous accordons une grande importance à notre communauté. Tous nos apprenants sur Seela et nos joueurs sur BattleHack se rassemblent sur notre serveur Discord, formant ainsi une véritable communauté. Cet espace est un lieu d'échange et d'entraide. Nous comptons sur eux pour nous faire part de leurs frustrations et signaler les bugs, car c'est ainsi que nous faisons vivre notre plateforme, qui est également la leur ! En tant que petite entreprise, nous avons l'avantage d'être réactifs, ce qui nous permet de corriger rapidement les problèmes et de continuer à nous améliorer. Cette proximité avec nos utilisateurs constitue également l'une de nos forces majeures.

Quels sont les principaux défis que vous avez rencontrés lors de la création et du développement de la plateforme ?

Pour évaluer si nous sommes sur la bonne voie et pour favoriser la communication entre les différentes équipes, il est essentiel que nos idées soient compréhensibles pour tous. En tant qu'entreprise jeune, Seela doit également prendre en compte les contraintes budgétaires, tout en proposant un produit supérieur à la concurrence.

Seela évolue sur un marché extrêmement compétitif où les deux géants américains ont déjà une forte présence, même sur le marché français. Nous avons donc décidé de nous démarquer en proposant une approche ludique, tandis que nos concurrents privilégient une approche plus traditionnelle.

Tests utilisateurs

Evaluer l'utilisabilité

Les test utilisateurs, c'est quoi ?

Les tests utilisateurs sont des méthodes d'évaluation dans lesquelles des utilisateurs interagissent avec un produit pour évaluer son utilisation et son expérience. Ils impliquent généralement un échantillon représentatif d'utilisateurs cibles, qui effectue des tâches spécifiques ou explore librement le produit pendant que des observateurs enregistrent leurs interactions, et commentaires. Les utilisateurs fournissent des données qualitatives et quantitatives utilisées pour guider les décisions de conception et optimiser l'expérience utilisateur.

Les tests utilisateurs permettent de valider les choix de conception, de détecter les problèmes et d'optimiser l'expérience. En impliquant les utilisateurs dès les premières étapes du développement, les tests contribuent à créer des produits plus adaptés aux besoins et attentes des utilisateurs finaux.

Les objectifs des tests utilisateurs

Implication
Réaliser des tests sur un échantillon cible

Evaluation
Comprendre comment l'utilisateur interagit

Evolution
Définir les améliorations possible de l'interface

Pourquoi les tests utilisateurs sont essentiels pour rendre la cybersécurité accessible à tous ?

Réaliser des tests utilisateurs permet d'identifier les obstacles et les difficultés que les utilisateurs peuvent rencontrer lors de l'utilisation de produits ou de services liés à la cybersécurité. En observant les comportements, les réactions et les feedbacks des utilisateurs, les tests permettent de comprendre leurs besoins, compétences et lacunes en matière de sécurité en ligne. Ces informations sont essentielles pour concevoir des solutions intuitives et adaptées, afin d'autonomiser les utilisateurs et de les aider à prendre des décisions éclairées en matière de sécurité numérique.

Les tests utilisateurs permettent de mieux comprendre leurs besoins et leurs attentes afin d'y répondre au mieux à travers une expérience simple et des fonctionnalités pertinentes.

Comment effectuer de bons tests utilisateurs ?

1

Définir des objectifs clairs

Avant de commencer les tests, identifiez clairement ce que vous souhaitez apprendre ou valider. Avoir des objectifs précis vous permettra de concentrer vos efforts et d'obtenir des résultats significatifs.

2

Recrutement des participants

Assurez-vous de sélectionner des participants qui correspondent à votre public cible. Ils doivent être représentatifs de vos utilisateurs réels afin d'obtenir des commentaires pertinents.

3

Concevoir des scénarios réalistes

Créez des scénarios qui simulent des situations réelles dans lesquelles les utilisateurs interagiront avec votre produit ou service. Les scénarios doivent être clairs, concrets et axés sur les tâches principales que vous souhaitez tester.

4

Réalisation des tests

Accueillez les participants, expliquez-leur le déroulement du test et observez attentivement leur comportement tout en prenant des notes. Vous pouvez également enregistrer les sessions pour une analyse ultérieure.

5

Encourager les retours honnêtes

Après chaque session, les participants doivent partager leurs impressions. Posez des questions ouvertes pour obtenir des informations détaillées sur leur expérience. Assurez-vous de créer un environnement où les participants se sentent à l'aise de partager leurs opinions négatives et positives.

6

Analyse et interprétations

Une fois les tests terminés, analysez les données collectées de manière approfondie. Identifiez les tendances, les problèmes récurrents et les points forts. Utilisez ces résultats pour prendre des décisions éclairées concernant les améliorations à apporter à votre produit ou service.

Les tests utilisateurs ne devraient pas être un processus ponctuel. Répétez régulièrement les tests tout au long du cycle de développement de votre produit ou service. Cela vous permettra d'itérer et d'améliorer continuellement votre solution en fonction des commentaires des utilisateurs.

Amélioration continue

Optimiser l’expérience utilisateur

L’amélioration continue, c’est quoi ?

L'amélioration continue est une démarche systématique et proactive visant à constamment améliorer l’expérience utilisateur. Elle implique de rechercher en permanence des opportunités d'optimisation, d'identifier les défauts, et de mettre en place des actions correctives. Les petites améliorations cumulées peuvent avoir un impact significatif sur la qualité, l'efficacité et la performance globale. Cela se fait de manière récurrente, en évaluant les résultats des améliorations précédentes, en apportant des ajustements et en continuant à élever les standards de performance.

L'amélioration continue favorise l'innovation, l'efficacité opérationnelle et la satisfaction, en répondant aux besoins changeants des clients, tout en renforçant la compétitivité en s’adaptant aux évolutions du marché.

Les objectifs de l’amélioration continue

Optimisation
Améliorer la performance globale et la qualité

Adaptabilité
Répondre efficacement aux besoins utilisateurs

Innovation
Processus créatif favorisant de nouvelles idées

Pourquoi l’amélioration continue est un outil clé pour rendre la cybersécurité accessible à tous ?

L’amélioration continue permet d'identifier et de résoudre les lacunes et les obstacles qui peuvent rendre la sécurité en ligne complexe ou intimidante. Elle vise à ajuster et améliorer en permanence l’expérience utilisateur pour répondre à leurs besoins changeants et aux nouvelles menaces. En appliquant des principes d'amélioration continue, les professionnels de la cybersécurité peuvent garantir un niveau de sécurité optimal et réduire les barrières à l'accessibilité. Elle favorise l'innovation, ce qui permet de développer de nouvelles approches et technologies pour rendre la cybersécurité plus conviviale, intuitive et facile à adopter, contribuant ainsi à protéger un plus grand nombre de personnes contre les menaces en ligne.

L'amélioration continue garantie une cybersécurité inclusive et évolutive, créant un environnement numérique sûr pour tous les utilisateurs, quelque soit leur niveau de compétence.

Quelle méthode appliquer pour effectuer de l'amélioration continue ?

Le cycle PDCA (Plan-Do-Check-Act)

01

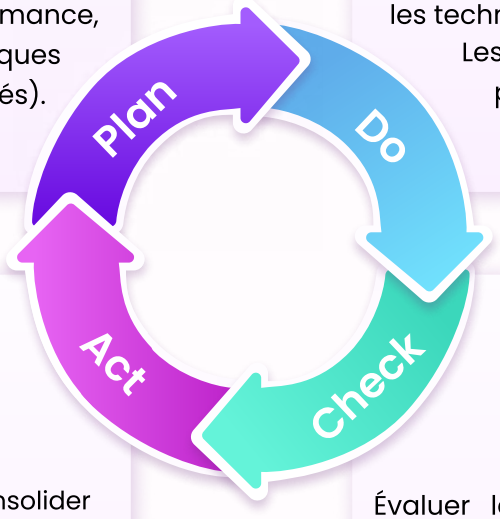
Plan (planifier)

Définir les objectifs d'amélioration, identifier les domaines à améliorer et établir un plan d'action (fixer des indicateurs de performance, d'établir des mesures spécifiques et de définir les responsabilités).

02

Do (faire)

Mettre en œuvre les actions planifiées (changements dans les processus, les méthodes de travail, les technologies ou les formations). Les actions sont mises en place de manière contrôlée.



04

Act (agir)

Prendre des mesures pour consolider les améliorations. Si les résultats sont satisfaisants, les actions peuvent être intégrées comme de nouvelles pratiques standard. Autrement, des ajustements sont apportés et le processus est répété.

03

Check (vérifier)

Évaluer les résultats des actions mises en œuvre (collecter et analyser les données pertinentes, comparer les résultats obtenus avec les objectifs fixés et évaluer l'efficacité des axes d'amélioration).

Pourquoi utiliser cette méthode ?

Cette méthode permet d'établir un processus d'amélioration en encourageant l'expérimentation, l'évaluation des résultats et l'ajustement constant des actions. Le cycle PDCA favorise l'optimisation de l'efficacité opérationnelle, la qualité, la productivité et la satisfaction client. Les utilisateurs contribuent activement à cette évolution en partageant leur retour d'expérience.
La méthode PDCA offre une approche structurée qui permet d'identifier les problèmes, de mettre en place des actions correctives, d'évaluer les résultats et d'apporter des ajustements en boucle pour favoriser l'innovation et la croissance.

Sensibilisation

Engager les utilisateurs

La sensibilisation, c’est quoi ?

La sensibilisation vise à informer et éveiller les consciences des individus sur une question spécifique ou une problématique donnée. En fournissant des informations pertinentes, des faits et des explications pour aider les personnes à comprendre les enjeux et les conséquences liés à la question abordée, l'objectif de la sensibilisation est d'encourager une prise de conscience et un changement d'attitude, en suscitant l'intérêt et l'engagement.

La sensibilisation permet d’éveiller les consciences, d'engager les individus et de favoriser des changements positifs en éduquant et mobilisant les gens autour de questions cruciales et de problématiques importantes.

Les objectifs de la sensibilisation

Education
Informer au mieux les utilisateurs

Engagement
Encourager la participation active

Accessibilité
Créer des supports faciles à comprendre

Pourquoi la sensibilisation est un outil clé pour rendre la cybersécurité accessible à tous ?

La sensibilisation permet aux individus de comprendre les différentes menaces auxquelles ils sont confrontés dans le monde numérique. En connaissant les risques, les utilisateurs peuvent adopter des comportements sécurisés pour se protéger. Ils prennent des décisions plus éclairées lorsqu'ils interagissent avec la technologie. Les utilisateurs jouent un rôle actif dans la protection de leurs données personnelles et de leur vie numérique. Ils apprennent à être prudents avec les informations qu'ils partagent en ligne et à la manière dont elles peuvent être utilisées par des tiers malveillants.

Des utilisateurs mieux informés et plus conscients des menaces sont moins susceptibles de tomber dans des pièges en ligne, ce qui limite la propagation des attaques et des cybercrimes.

Comment mettre en place une campagne de sensibilisation efficace ?

Les éléments clés d'une sensibilisation réussie

Définir l'objectif

Déterminez des objectifs clairs de votre campagne de sensibilisation. Quels sont les résultats que vous souhaitez atteindre ? Souhaitez-vous informer les utilisateurs sur les risques associés à la sécurité en ligne ou encourager l'adoption de bonnes pratiques pour une meilleure sécurité ? Définissez des objectifs précis et mesurables afin de guider vos actions de manière ciblée et évaluer votre progression.

Analyser la cible

Vous devez comprendre votre public cible, identifiez les caractéristiques démographiques, les connaissances préalables, les comportements actuels et les besoins spécifiques de votre public. Cette analyse approfondie vous permettra d'adapter votre message et vos stratégies de communication en fonction des attentes et des motivations de votre public, afin de maximiser l'impact de votre campagne de sensibilisation.

Concevoir le message

Le sujet de cybersécurité semble complexe, ce qui rend réticent les utilisateurs. Utilisez un langage simple et accessible pour transmettre les informations clés. Mettez l'accent sur les avantages de la sécurité en ligne et les conséquences négatives des comportements risqués. Utilisez des exemples concrets et des anecdotes pour rendre le message plus concret.

Choix canaux de communication

Choisissez les canaux de communication les plus pertinents pour atteindre votre public cible. Les différents canaux permettent une diversité de format attractif pour retenir l'utilisateur et favoriser son engagement. Grâce à des formats visuels comme la vidéo ou interactif comme les quizz en story sur les réseaux on peut impliquer l'utilisateur et ainsi rendre le message plus impactant.

Impliquer les parties prenantes

Les utilisateurs étant la première faille de sécurité en informatique, il est essentiel de collaborer avec des parties prenantes, telles que les RSSI, les équipes de communication interne, les employés et les gestionnaires. Impliquez-les dans la planification et l'exécution de la campagne pour maximiser son impact. Assurez-vous de fournir des ressources, des outils et un soutien adéquat aux parties prenantes impliquées.

Evaluer et ajuster

Évaluez l'efficacité de votre campagne de sensibilisation en mesurant les résultats par rapport aux objectifs définis. Utilisez des indicateurs clés de performance tels que la participation, la compréhension et les feedback utilisateurs. Sur la base de ces résultats, ajustez et améliorez votre campagne en apportant des modifications appropriées pour assurer une amélioration continue.

Formation

Eduquer les utilisateurs

Une formation, c’est quoi ?

La formation est un processus d'apprentissage organisé et structuré qui vise à acquérir un nouveau savoir, développer des compétences spécifiques et améliorer les performances dans un domaine donné. Son objectif principal est de préparer les apprenants à relever les défis et les opportunités de leur environnement, en favorisant leur développement personnel et professionnel. Par le biais de programmes de formation, elle offre aux individus les outils et les aptitudes nécessaires pour réussir et s'adapter dans un monde en constante évolution.

La formation est un moyen essentiel pour acquérir les connaissances et les compétences nécessaires afin de prospérer dans différents domaines de la vie.

Les objectifs de la formation

Apprentissage
Enseigner aux utilisateurs les acquis nécessaires

Changer les habitudes
Encourager l’adoption des bonnes pratiques

Responsabilisation
Autonomiser en fournissant les outils adéquates

Pourquoi la formation est un outil clé pour rendre la cybersécurité accessible à tous ?

Aujourd’hui, tout le monde possède une vie numérique, pourtant on ne sait pas tous la protéger correctement. Le sujet de la cybersécurité est complexe, il demande des connaissances et compétences techniques qui semblent inaccessibles pour beaucoup de gens, notamment auprès des plus jeunes qui ont toujours connu les écrans. Les principales vulnérabilités venant des utilisateurs, il est essentiel de les former aux bonnes pratiques et aux menaces potentielles afin qu’ils puissent s’en protéger au mieux et ainsi assurer la sécurité de leur écosystème numérique.

Former les utilisateurs à la cybersécurité, c'est leur donner les clés pour naviguer en ligne en toute confiance, comprendre les risques et leur fournir les acquis nécessaires pour prendre des décisions éclairées pour se protéger.

Comment former efficacement les utilisateurs ?

1

Définir des objectifs clairs

La formation doit définir des objectifs d'apprentissage bien définis et alignés sur les besoins des apprenants et les résultats attendus. Ils servent de guide pour structurer le contenu et les activités de formation.

2

Pertinence et adaptabilité

La formation est pertinente pour les apprenants et leur domaine d'application. Elle doit prendre en compte les connaissances et les compétences préalables des participants et s'adapter à leurs besoins spécifiques.

3

Engagement actif

La formation encourage l'engagement actif des apprenants. Elle doit impliquer les participants dans des activités pratiques, des études de cas, des discussions et des exercices interactifs. L'interactivité favorise l'apprentissage actif, la réflexion critique et l'application pratique des connaissances.

4

Feedbacks constructifs

La formation intègre des feedbacks réguliers et constructifs. Les formateurs fournissent un retour d'information aux apprenants sur leurs progrès, leurs erreurs et leurs points forts. La rétroaction encourage l'amélioration continue et permet aux participants de s'auto-évaluer et de s'ajuster en conséquence.

5

Evaluation de l'apprentissage

La formation comprend des évaluations formelles et informelles pour mesurer les progrès des apprenants. Elle permet de vérifier si les objectifs d'apprentissage sont atteints et d'identifier les domaines qui nécessitent un renforcement supplémentaire.

6

Suivi et soutien continu

Une formation efficace ne se limite pas à un événement ponctuel, mais offre un suivi et un soutien continu après la fin de la formation. Ils assurent une application durable des connaissances acquises et un soutien continu aux apprenants.

03

En pratique

Maintenant que nous avons tous les outils pour rendre plus compréhensible les sujets de la cybersécurité, nous allons voir comment ils peuvent être appliqués concrètement. Découvrons comment Phinasoft rend la cybersécurité plus accessible grâce à ces astuces et comment je les ai accompagnés à travers mes missions.

Phinasoft

Présentation

Phinasoft est une start-up né en 2022, de l'expérience du terrain et d'un constat : une dépendance forte, dans l'écrasante majorité des organisations, vis-à-vis des fichiers excel pour la réalisation des analyses de risques, la gestion d'un SMSI, le suivi ou le reporting. Cela représente une perte de temps et d'efficacité majeure pour les équipes SSI et fait partie intégrante de la difficulté à impliquer les collaborateurs.

Est-ce que l'on imaginerait aujourd'hui, au-delà d'un certain seuil, une équipe commerciale sans CRM ou une équipe comptable sans ERP ?
C'est pourtant encore la réalité pour les équipes de cybersécurité.

Phinasoft apporte enfin la solution pour que vous puissiez vous concentrer sur votre métier : la sécurité.

Phinasoft est une solution de Management des risques de Cybersécurité permettant à votre entreprise d'avoir une vision de ses risques claire et ancrée dans ses enjeux et objectifs. Elle facilite l'intégration du risque cyber dans la prise de décision à tous les échelons de l'entreprise. Elle est totalement modulable aux spécificités de votre contexte organisationnel et technique.

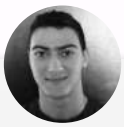
Grâce à phinasoft

- Les équipes métiers intègrent plus facilement dans leurs décisions les risques de sécurité de l'information
- Les équipes sécurité passent plus de temps sur leur cœur de métier : la sécurité
- La collaboration entre équipes métiers et techniques est largement facilitée
- La gestion du risque cyber et ses méthodes trouvent l'outillage idéal sur lequel s'appuyer

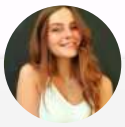
Présentation de l'équipe

Guillaume ALLIEL
CEO
Enseigne la cybersécurité à HEC Paris et accompagne les entreprises sur leur gouvernance SSI. Il est diplômé de HEC Paris.

Adrien ALLIEL
CIO
Développeur Full-Stack avec une riche expérience de Management d'équipes IT et UX, diplômé d'EPITECH.



Chai BITTAN
CTO
Développeur Full-Stack aguerri au service de startups comme de grands groupes. Il est diplômé d'EPITECH.



Amandine FULOP
UX/UI et stratégie digitale
En cours d'obtention d'un mastère Expert stratégies digitales à l'ESD, UX/UI designer et chargée de projet digital.

Et en pratique ?

Comment Phinasoft rend la cybersécurité plus accessible grâce à ces astuces ?

Phinasoft en 2021

Phinasoft avait déjà une stratégie digitale en place : un produit pensé pour facilité la vie de ses utilisateurs (étant destiné à des professionnels n'ayant pas nécessairement de compétences cyber, l'information est adaptée au niveau des utilisateurs), un site vitrine pour mettre en avant cette plateforme et récolter les e-mails de prospects et une communication LinkedIn pour accroitre la visibilité. Cependant, l'existant était assez minimaliste et pouvait être amélioré.

Logo et identité
L'impact visuel du logo pouvait être amélioré et modernisé avec une simplification de la lecture et la visibilité, surtout à distance et des couleurs plus dynamiques.

Site internet
Le site web one-page pouvait être restructuré en différentes pages distinctes pour faciliter la navigation et rendre l'expérience plus agréable pour les visiteurs.

Post LinkedIn
Pour la communication sur LinkedIn, il serait bénéfique de développer une identité visuelle claire permettant de reconnaître Phinasoft au premier coup d'œil.

Plateforme Phinasoft
La console Phinasoft, offre déjà une expérience utilisateur convaincante. Toutefois, il pourrait être intéressant d'enrichir la plateforme avec plus d'éléments visuels.

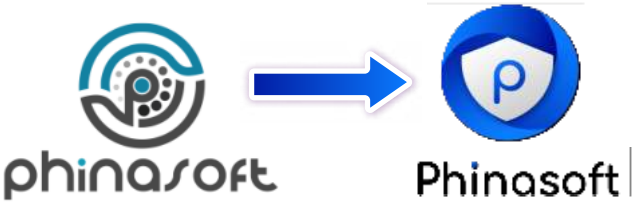
Phinasoft a déjà établi une solide base pour tous leurs supports digitaux. **En rafraîchissant la charte graphique du site on peut lui donner un aspect plus dynamique et attrayant, pour renforcer l'impact visuel global et optimiser l'impact sur les utilisateurs.**

Les actions menées

Charte graphique

L'objectif était de conserver les formes arrondis, organiques qui évoquent la fluidité, l'accessibilité et donnent un sentiment de confiance, tout en apportant un nouveau dynamisme et une réelle signification. **On retrouve la roue qui évoque l'évolution, le bouclier pour la sécurité et la clé pour inspirer une solution clé en main.**

La charte graphique définie les couleurs, les typos, les règles de conception. Elle guide la création de l'ensemble des supports de communication pour **assurer une cohérence visuelle et renforcer l'identité de marque de Phinasoft**



Refonte du site internet

Le site web est au centre de la communication digitale, c'est l'un des premiers points de contact avec les utilisateurs.
On y trouve des informations sur l'entreprise, le produit, les cas d'usages, qui permettent de renseigner l'usager sur l'intérêt d'analyser et gérer les risques cyber. Il était important de structurer l'information avec une arborescence intuitive offrant une navigation fluide et une bonne accessibilité.
L'expérience utilisateur, le design d'interface, les interactions et le niveau de langage adapté à la cible ont permis la conception de ce site qui met en avant Phinasoft et l'analyse de risques.

Création du blog

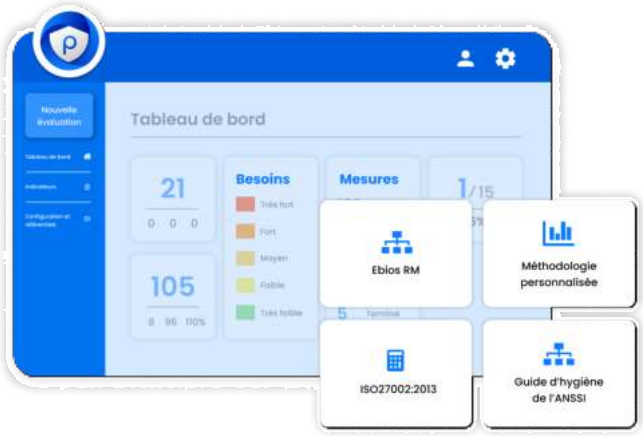
Depuis la refonte du site, nous avons mit en place un blog afin de renforcer la sensibilisation aux sujets de la cybersécurité. Il permet de rendre accessible des sujets techniques comme le phishing en utilisant un langage adapté ou des supports visuels. La cybersécurité est un sujet large en constante évolution, grâce au blog on peut proposer des mises à jour constantes de l'information mais aussi des thématiques variées selon les besoins spécifiques. (Et en plus, c'est nécessaire pour un bon SEO !)

Post LinkedIn

Le compte LinkedIn est régulièrement alimenté et illustré par la présence aux salons et conférences, de nouveaux partenariats etc... Cependant la page de l'entreprise manquait d'engagement et l'absence de reconnaissance visuelle de Phinasoft était sûrement en cause. En proposant des templates de posts conçu selon la charte graphique, les visuels renforcent l'identité graphique de la marque.
Une meilleure identification permet d'optimiser la délivrance du message à la cible. On a la possibilité de faire des liens avec le site particulièrement en faisant la promotion des articles de blog.
Grâce à la communication LinkedIn, Phinasoft peut s'adresser à tous les utilisateurs et non seulement aux professionnels de la cyber.

Transformation visuelle de la console

La plateforme ayant déjà une bonne expérience utilisateur, il fallait surtout faire une refonte visuelle. Les informations essentielles et chiffrées seront illustrées avec des graphiques, des éléments colorés pour mettre en avant les niveaux de risques. L'ajout d'icônes rend plus visibles et distinctifs certains composants pertinents et utiles à la compréhension des utilisateurs. La hiérarchisation de l'information était déjà bien structurée. Toutefois, mettre plus en avant les sections, les titres, les tableaux et formulaires **optimisera la clarté, l'ergonomie et l'accessibilité de la plateforme Phinasoft.**



Et pour la suite ?

1

Plateforme

Les modifications offrant une meilleure expérience utilisateur seront intégrées d'ici 2024

2

Blog

Régulièrement l'enrichir d'articles sur les sujets cyber avec des contenus informatifs pertinents

3

Linkedin

Maintenir une présence active et interagir avec la communauté pour cultiver un fort engagement

4

Amélioration continue

Appliquer à tous nos outils et supports de communication, pour offrir une expérience optimale.

En résumé

Les astuces mises en place par Phinasoft

- Expérience utilisateurs (UX)
- Interface utilisateurs (UI)
- Langage adapté
- L'interactivité
- L'amélioration continue
- La sensibilisation
- La formation

L'impact de ces transformations sur l'accessibilité

Ces outils de communication rendent les sujets complexes plus accessibles pour un large public. L'identité visuelle cohérente et attractive renforce le professionnalisme de Phinasoft, suscitant ainsi la confiance des clients potentiels. La refonte du site web optimise l'expérience utilisateur en utilisant une mise en page épurée et des éléments visuels minimalistes pour faciliter la compréhension du contenu lié à la cybersécurité. Le blog et les templates LinkedIn fournissent des contenus clairs, concis et pratiques, aidant les lecteurs à mieux comprendre les enjeux de la cybersécurité et à prendre des mesures appropriées pour se protéger. Enfin, l'utilisation d'infographies et de visualisations de données permet aux informations de Phinasoft d'être plus digestes et accessibles, facilitant la compréhension des statistiques et des tendances clés en matière de risques cybernétiques. La charte graphique établit une identité visuelle forte, renforçant la crédibilité de l'entreprise et la reconnaissance de la marque par les utilisateurs. **Dans l'ensemble, ces outils de communication démocratisent le sujet de la cybersécurité en le rendant accessible à tous.**

Conclusion

La conception UX/UI : un levier essentiel pour rendre la cybersécurité accessible à tous

La cybersécurité est un enjeu qui concerne tout le monde, que ce soit les individus, les entreprises ou les institutions. Il est crucial d'impliquer tous les acteurs dans la **sensibilisation et la prise de mesures pour garantir un environnement en ligne sûr et protégé**. Pour rendre la cybersécurité accessible à tous, nous avons des **astuces de conception pour créer des interfaces intuitives et engageantes**.

Ces astuces de conception UX/UI présentées vous donnent les clés pour créer d'interfaces qui **facilitent la compréhension et l'adoption des bonnes pratiques** de cybersécurité. En simplifiant les informations complexes, en utilisant des visuels accrocheurs et en fournissant des rétroactions claires, nous pouvons aider les utilisateurs à mieux comprendre les risques et les mesures de protection. **Des interfaces conviviales et ergonomiques encouragent également l'engagement des utilisateurs, renforçant ainsi leur adhésion aux bonnes pratiques de sécurité.**

Cependant, la conception UX/UI ne se limite pas à la création d'interfaces attrayantes. Il est important de **se tenir informé des évolutions technologiques et des nouvelles tendances en matière de cybersécurité**. La nature changeante des menaces nécessite une adaptation constante de nos stratégies de conception pour **répondre aux besoins des utilisateurs et aux défis émergents**. En gardant une mentalité ouverte et en restant à l'écoute des retours des utilisateurs, nous pouvons **continuellement améliorer les interfaces et les expériences pour renforcer la sécurité en ligne**.

La cybersécurité est une responsabilité collective qui nécessite la participation active de tous les acteurs. En utilisant les astuces de conception UX/UI pour rendre ce sujet complexe plus accessible, nous pouvons créer des interfaces intuitives et engageantes qui favorisent l'adoption des bonnes pratiques de sécurité. Cependant, cela ne s'arrête pas là. Nous devons rester vigilants, nous adapter aux évolutions technologiques et continuer à améliorer nos approches pour créer un environnement en ligne sécurisé et convivial pour tous.

Merci !

Avant de conclure ce livre blanc, je tiens à exprimer ma profonde gratitude envers les personnes qui ont contribué à sa réalisation et à mon parcours dans le domaine de l'UX UI design et de la stratégie digitale. Leur soutien, leur expertise et leur générosité ont grandement enrichi cette expérience.

Tout d'abord, je tiens à remercier chaleureusement Guillaume et Adrien Alliel ainsi que Chai Bittan, pour m'avoir accueillie chez Phinasoft, en alternance pendant deux années intenses. Leur mentorat, leurs conseils éclairés et leur collaboration ont été des piliers essentiels de ma croissance professionnelle. Je suis reconnaissante de leur confiance et de l'opportunité qui m'a été offerte de travailler à leurs côtés.

Je souhaite aussi remercier sincèrement Alexis Guittet et Hélène Batard de chez Seela pour cette interview passionnante sur la gamification de BattleHack. Nous avons partagé ensemble un moment privilégié, riche en échanges et en apprentissage. Leur engagement et leur vision ont parfaitement illustré les concepts abordés dans ce livre blanc.

Je voudrais remercier mon école, l'ESD, pour m'avoir donné l'opportunité de suivre cette formation enrichissante. Les enseignants et le personnel pédagogique ont joué un rôle essentiel dans mon développement professionnel, en me fournissant des connaissances solides et en me guidant dans mon apprentissage.

Enfin, je tiens à exprimer ma reconnaissance envers toutes les personnes qui ont contribué de près ou de loin à l'élaboration de ce livre blanc. Vos encouragements, vos idées et votre soutien indéfectible ont été d'une valeur inestimable pour moi.

Sources

Cybersécurité et astuces

https://www.lexpress.fr/economie/high-tech/a-5-ans-il-decouvre-une-faille-de-securite-de-la-xbox-one_1506290.html

https://www.kaspersky.fr/blog/cyber-securite-des-enfants-une-priorite-presente-et-future/

https://www.stoik.io/cybersecurite/chiffres-cles

https://www.cybersecurity-business.school/que-dit-la-loi-sur-la-cybersecurite/

https://www.verizon.com/business/fr-fr/resources/reports/dbir/

https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd#

https://lagrandeourse.design/blog/actualites/les-nouvelles-metriques-google-pour-une-bonne-ux/

https://www.sales-hacking.com/post/statistiques-cyberattaques

https://www.fevad.com/les-chiffres-cybercriminalite/

https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage

https://www.axido.fr/decouvrez-le-rapport-des-cyber-attaques-2022/

https://www.ssi.gouv.fr/actualite/le-rapport-dactivite-2022-de-lanssi-est-en-ligne/

https://esokia.com/fr/blog/ux-ui-quest-ce-que-ca-signifie

https://www.beedeez.com/fr/blog/tout-ce-que-vous-devez-savoir-sur-la-gamification

https://blog.hubspot.fr/marketing/storytelling

Illustrations et images

https://www.freepik.com/

https://iconify.design/

Rédigé par
Amandine FULOP