LIVRE BLANC

Olfeo
La sécurité positive

Responsabiliser vos utilisateurs

Non, le problème n'est pas entre la chaise et le clavier, c'est plutôt un levier de protection qu'il faut désormais activer !

SOMMAIRE

Olfeo
La sécurité positive

LE NOUVEAU DÉFI DE LA CYBERSÉCURITÉ EST-IL CELUI QUE L'ON CROIT ?

Pour faire face à la recrudescence des cyber menaces, les entreprises et les collectivités publiques ont pris conscience de la nécessité de mieux se protéger et de renforcer leur chaîne de sécurité. Il en résulte depuis plusieurs années une « course à la protection technologique », mais est-ce vraiment le seul enjeu ?

Car de l'autre côté, les hackers et cybercriminels le savent et s'adaptent en conséquence. Si détecter une faille dans le réseau informatique demande de plus en plus des compétences techniques avancées, la nouvelle tendance est assurément de profiter du « maillon faible ». C'est pour cela que l'on assiste régulièrement à la propagation de ransomwares et autres opérations de phishing qui ciblent les utilisateurs finaux et leur éventuelle inattention ou faiblesse.

D'ailleurs, on dit souvent qu'en termes de cybersécurité, le problème est entre la chaise et le clavier : mais est-ce vraiment un problème ? Ou plutôt un moyen de protection sous-exploité ?

Bien que de nombreuses études montrent que l'écrasante majorité des incidents de sécurité sont dus à des erreurs humaines, le vrai problème est que l'on fait face à un décalage de vision :

- D'un côté, les experts en sécurité des systèmes d'information reprochent aux utilisateurs finaux de ne pas respecter les principes de base de la sécurité ; les obligeant à augmenter constamment le niveau des outils de sécurité mis en place.
- De l'autre, les utilisateurs finaux se retrouvent confrontés à des menaces dont ils ne soupçonnent pas l'existence et face auxquelles ils peuvent commettre des erreurs rendant ainsi le système d'information extrêmement vulnérable à leur insu.

2 visions différentes et 2 équipes qui s'opposent alors qu'elles ont les mêmes aspirations : être protégées. Il est donc urgent que les organisations privées et publiques travaillent à développer une meilleure culture de la sécurité pour faire changer les comportements, créer de nouveaux réflexes de méfiance pour que les bonnes pratiques deviennent davantage spontanées.

> **Pour cela, il est fondamental de considérer l'implication des utilisateurs finaux comme un des nouveaux leviers d'amélioration de la cybersécurité !**

C'est dans cet esprit que nous avons créé cet Ebook, pour vous aider à mieux comprendre l'évolution des cyber menaces et les enjeux autour de la sensibilisation des utilisateurs afin de **transformer le facteur humain en un maillon fort de votre chaîne de sécurité.**

L'ÉVOLUTION DES CYBER MENACES

Quand on regarde l'évolution de la nature des cyber menaces, **force est de constater à la fois leur généralisation ainsi que leur professionnalisation…**

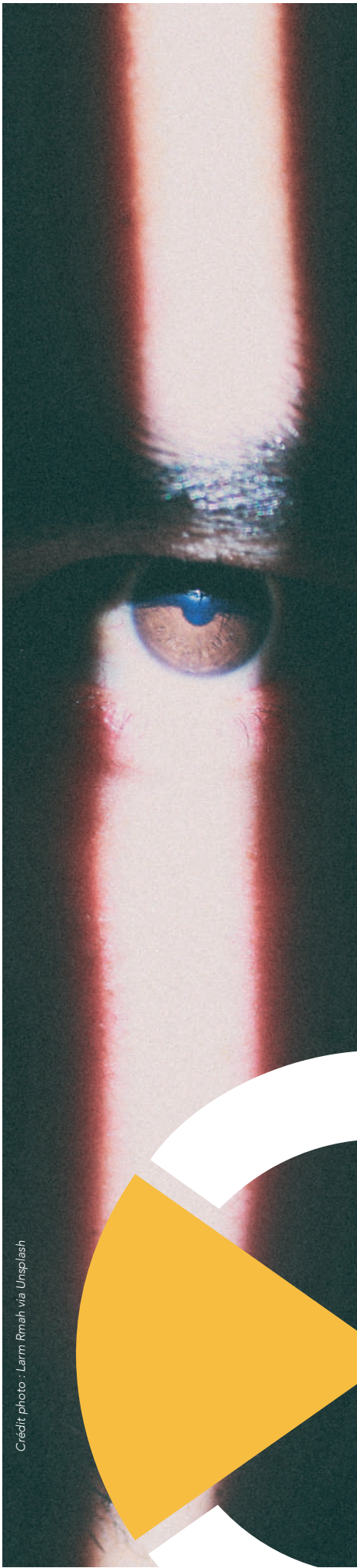
Les attaquants ne sont plus obligatoirement les développeurs des malwares et l'on assiste aujourd'hui au développement d'une véritable économie autour des attaques. En effet, il est désormais très facile de louer des kits de ransomwares sur les places de marché les plus populaires du Darknet. Certains kits bénéficient même d'un véritable marketing vantant la simplicité d'usage, la dimension « Do It Yourself » car plus aucune compétence de codage n'est requise voire même présentant des éléments prévisionnels de ROI !
On découvre ainsi le « Ransomware as a Service ».

Ces attaques plus « artisanales » qui se généralisent semblent malgré tout **faire moins de dégâts que des attaques provenant d'organisations criminelles professionnalisées qui vont chercher à exploiter simultanément les failles systèmes et le facteur humain.** Ces cybercriminels construisent ainsi des stratégiques d'attaques personnalisées : ils collectent de l'information, identifient leurs interlocuteurs grâce aux informations disponibles sur le web et les réseaux sociaux puis contextualisent leurs attaques.

Les opérations de phishing sont ainsi de plus en plus élaborées : aucune faute d'orthographe, un design graphique strictement identique aux communications officielles de l'organisme usurpé et des mentions contextualisées parfois personnelles mais souvent pertinentes trompant la vigilance de l'utilisateur qui clique sur une URL malveillante...

L'enjeu de ces attaques est de maximiser les résultats en un minimum de temps. Elles cherchent donc à exploiter simultanément différents supports comme le mobile ou les réseaux sociaux avec les fausses invitations à se connecter comme c'est régulièrement le cas avec Facebook et LinkedIn. Leurs objectifs vont du simple clic sur l'URL malveillante qui va chercher à télécharger un ransomware jusqu'à la récupération du mot de passe d'un interlocuteur ciblé. Cela permet aux cyber criminels d'utiliser la technique du « Spoofing » dont l'objectif est de pirater sa messagerie pour envoyer des emails en usurpant son identité dans le cadre d'une opération de piratage plus élaborée.

L'ingénierie sociale des cyber menaces s'est donc généralisée et professionnalisée afin d'exploiter les techniques élémentaires de manipulation pour faire en sorte que les personnes se conforment aux souhaits des attaquants. Les équipes en charge de la sécurité des systèmes d'informations assistent ainsi à l'explosion du nombre d'attaques cherchant à exploiter les faiblesses de la nature humaine et pour lesquelles elles ne disposent pas toujours du temps suffisant pour réagir avant que la menace réussisse à pénétrer le réseau informatique.


Crédit photo : Larm Rmah via Unsplash

LE FACTEUR HUMAIN ET LES 7 PÉCHÉS CAPITAUX

Si la recherche du sentiment de sécurité est inhérente à la nature humaine, elle peut parfois être en décalage total avec la réalité et tout le monde ne dispose pas d'un sixième sens pour pressentir le danger, d'autant plus en matière de cybersécurité !

Les cybercriminels le savent et exploitent désormais la plupart des 7 péchés capitaux dans leurs attaques ! La peur, le stress, la convoitise, la paresse… font désormais partie des plans d'attaque avec toujours cet objectif d'aller vite pour ne pas laisser le temps au sixième sens ou aux équipes informatiques de réagir. La demande est extrêmement pressante, on doit répondre dans l'urgence et les attaquants créent le stress nécessaire.

Les victimes sont toujours démunies face à la sophistication des attaques et aux approches psychologiques utilisées. Après un clic dans un email de phishing, un utilisateur peut recevoir un coup de téléphone et le cyber criminel peut essayer de le manipuler en jouant sur la peur et la responsabilité : « si vous ne le faîtes pas, votre chef vous en tiendra responsable… », la culpabilité : « Vous ne voulez pas m'aider ? Je pensais que vous étiez quelqu'un de bien… » ou encore la cupidité : « Si vous m'aidez, vous en retirez un grand bénéfice… ».

2 Questions à notre expert

Franck Gicquel
Responsable des partenariats
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Comment voyez-vous l'évolution des cyber menaces ?

« Nous avons réellement franchi un cap en termes de professionnalisation des attaques sur le fond comme sur la forme : plus de fautes d'orthographe, les créations graphiques des emails de phishing sont remarquables et contextualisées par rapport aux périodes comme on l'a vu pour le Black Friday. Mais surtout, nous assistons à la convergence des menaces digitales et physiques. Les attaquants sont de plus en plus structurés pour contourner les moyens de défense et jouer un billard à 3 bandes : digital, temps réel et démultiplication des attaquants. »

Comment réagir dans ce cas ?

« Il faut évidemment évangéliser davantage les utilisateurs sur la réalité et les caractéristiques des menaces aujourd'hui. C'est de l'ordre de la responsabilité de l'entreprise d'apprendre aux utilisateurs à être plus fort mais la 1ère chose à faire est de démystifier le sujet : lorsque les DSI et RSSI passent des consignes, cela peut être perçu comme juste de nouvelles contraintes s'ajoutant à la liste… Il faut revenir aux fondamentaux en leur parlant d'abord des usages dans leur vie personnelle si l'on veut réussir à les impliquer davantage puis à les rapprocher avec les enjeux de sécurité business. C'est pour cela que Cybermalveillance.gouv.fr met à disposition son kit de sensibilisation des collaborateurs composé autour d'outils ludiques… »

LA SÉCURITÉ, C'EST L'AFFAIRE DE TOUS

Pour faire face à tant de sophistication mais aussi d'incertitudes, **on ne peut plus douter que la sécurité soit réellement l'affaire de tous** : des éditeurs de logiciels, des pouvoirs publics, de la direction générale, de la DSI et bien sûr des utilisateurs finaux ! Personne n'a oublié la version piratée du logiciel CCleaner en Août 2017 qui a infecté 700.000 personnes dans le monde et parmi lesquelles des entreprises comme Google, Microsoft ou Samsung.

Cela n'arrive pas qu'aux autres ! Même si de nombreux outils de sécurité ont été mis en place dans l'organisation, **il est désormais vital que les utilisateurs se sentent également responsables**. D'ailleurs, le risque d'une politique de sécurité trop restrictive ou qui entrave les besoins des utilisateurs est parfois de pousser à avoir des comportements de contournements, voire même volontairement nuisibles (installation d'un VPN sur le poste, etc.), plutôt que d'encourager à réagir de la manière appropriée.

C'est d'autant plus important que l'on passe désormais du phishing autour de l'offre promotionnelle à des arnaques exploitant simultanément le monde numérique et la vie réelle. Comme par exemple celles du faux support technique, combinant emails et téléphones, dont plusieurs milliers de cas ont été recensés en France ces derniers mois. La technique est simple : la victime est contactée par SMS, téléphone ou email pour lui signaler un problème sérieux sur son équipement informatique et lui demander de contacter un faux support technique, sous peine de perdre toutes ses données ou de ne plus pouvoir utiliser son matériel. La vitesse de réaction face à une attaque devient donc le point clé et se joue autant au niveau de l'utilisateur final que des outils informatiques.

Dès lors, la sensibilisation aux nouvelles cyber menaces devrait déjà être généralisée dans toutes les organisations et surtout à tous les niveaux. Elle ne peut plus se limiter uniquement à la signature obligatoire de la charte informatique lors de l'intégration d'un nouveau collaborateur !

Un exemple concret concerne évidemment la gestion des mots de passe : la quasi-totalité des chartes informatiques exigent désormais des mots de passes « compliqués » avec des majuscules, minuscules, chiffres voire caractères spéciaux… Cela n'empêche pas malgré tout que « Password1 », « P@ssword1 » ou « Nomdel'entreprise01 » soient les mots de passe les plus répandus et souvent utilisés à plusieurs endroits. Les hackers le savent et les ont déjà intégrés dans leurs routines de connexion. Par contre, de l'autre côté, combien d'utilisateurs le savent vraiment ?

Cela fait trop longtemps que sensibiliser l'utilisateur final a été négligé dans les politiques de sécurité des entreprises comme des collectivités publiques. **Il faut aujourd'hui engager un véritable changement de mentalité** : la DSI ne doit plus vouloir bloquer ni occulter le facteur humain par la technologie mais plutôt l'accompagner, le faire évoluer si elle veut le transformer en un maillon plus fort de sa chaîne de sécurité.

Crédit photo : Smugglers Lair via Unsplash

ARRÊTER DE SE FAIRE PEUR POUR FAIRE CHANGER LES COMPORTEMENTS

Faire changer les comportements commence parfois par soi-même et la DSI n'échappe pas à la règle. En effet, sensibiliser ne veut pas dire « spammer » les utilisateurs d'alertes de sécurité, de nouvelles règles ou de nouvelles contraintes. **La DSI ne doit plus chercher à « maîtriser » le facteur humain ou à « faire peur » aux utilisateurs mais plutôt à les impliquer davantage pour les responsabiliser**. Pour cela, il est fondamental d'associer à la fois la communication sur les risques encours avec les bonnes pratiques en termes de réaction si l'on veut créer une prise de conscience.

C'est par contre un projet que la DSI ne peut pas mener seule. En effet, **cela exige d'engager une démarche d'évangélisation intégrée dans la communication globale de l'entreprise**. La DSI aura donc besoin de s'associer à d'autres services comme la communication interne ou les ressources humaines dans les PME… Mais pour que cette nouvelle synergie interservices soit réellement efficace, il doit obligatoirement y avoir une implication de la direction générale dans la démarche. L'exemple doit venir d'en haut si l'on veut que la prise de conscience autour de la sécurité soit un vrai sujet dans l'entreprise.

2 Questions à notre expert

Farid Agha
Directeur Customer Success
Olfeo
La sécurité positive

Comment pensez-vous que l'on peut changer les comportements ?

« Une erreur courante lorsqu'une organisation souhaite engager une démarche de sensibilisation est de continuer à considérer l'utilisateur comme un problème. Dans ce cas, les messages resteront anxiogènes et donc mal perçus par les utilisateurs finaux. Au contraire, si l'on veut créer une culture de la sécurité qui soit réellement positive, il est indispensable de considérer l'utilisateur final comme un composant essentiel de la performance de la chaîne de sécurité en lui diffusant par exemple des messages pertinents et adaptés au contexte de ses usages informatiques. »

Comment contribuez-vous à responsabiliser les utilisateurs chez Olfeo ?

« Nos solutions sont basées sur le concept de la sécurité positive et nous considérons chaque personne comme un utilisateur responsable que l'on cherche à impliquer. Leur vigilance et leur capacité d'action sont essentielles pour la sécurité de l'organisation. Notre passerelle de sécurité web permet ainsi d'interagir avec eux grâce à des messages explicites misant sur leur bon sens et leur capacité de prise de recul en les informant de la nature du lien sur lequel ils viennent de cliquer par exemple. Notre objectif est de les rendre ensuite plus vigilants avant de cliquer… ».

LES 3 FONDAMENTAUX POUR RÉUSSIR VOS ACTIONS DE SENSIBILISATION

Lorsque les utilisateurs comprennent mieux les risques encourus, ils sont plus à même de détecter des comportements suspects ou d'adopter une plus grande prudence face à un site web d'apparence officielle qui leur demanderaient des informations sensibles… Diffuser une meilleure culture de la sécurité dans l'organisation permet ainsi de créer une véritable prise de conscience chez chaque individu.

Cela demande un effort régulier dans ses actions ainsi qu'une plus grande simplicité de la part de la DSI.
En matière de sécurité, une bonne pédagogie ne se résume pas qu'à informer, il est indispensable de mettre en place des exercices ou des simulations qui vont créer cette prise de conscience par l'exemple. Ces bonnes pratiques sont souvent ludiques, avec des quizz de mise en scène pour les collaborateurs ou des simulations d'opérations de phishing qui vont permettre de mesurer l'évolution des réactions en interne.

Dans tous les cas,
il est important de respecter
3 fondamentaux pour réussir
vos actions de sensibilisation :

1

La récurrence

La récurrence est le point clé : sensibiliser une fois de temps en temps n'est pas efficace. **Il faut définir une véritable stratégie de communication continue**, appuyée par la direction générale comme mentionné précédemment et dont les différentes actions seront planifiées dans le temps et connues de tous. Il faut également multiplier les canaux de diffusion ainsi que les formats de contenus : des webinaires internes, des réunions en présentiel, des quizz ou vidéos, des informations de sensibilisation lors de leur navigation internet. L'information apparaît ainsi au bon endroit, au bon moment, de manière contextualisée. **Tout ce qui est interactif fonctionne beaucoup mieux aujourd'hui mais il ne faut pas oublier d'y mettre de l'humain** : un utilisateur ne pourra jamais se former tout seul devant sa machine et maîtriser tous les risques.

2

S'adapter aux différents interlocuteurs

Les experts de la sécurité considèrent de nombreuses choses comme « acquises » ou agissent de la bonne manière mais de façon inconsciente. Ce n'est pas le cas chez tous les utilisateurs. Chaque être humain ne va pas forcément être réceptif au même type de message, **toute action de sensibilisation devra donc avoir plusieurs niveaux d'expertise sur les sujets traités** : du très basique pour rendre accessible des informations compliquées à un public très large jusqu'au plus avancé pour ceux qui souhaitent aller plus loin et devenir des référents internes. Il est illusoire de croire que les utilisateurs finaux vont s'engager et apprendre si l'on utilise des supports de communication élitistes et complexes.

C'est pour cela que **beaucoup d'organisations se tournent également vers des actions de coaching, tant humaines que technologiques**. Le coaching facilite en effet la sensibilisation contextuelle, c'est-à-dire au moment où l'erreur est potentiellement commise : il est beaucoup plus efficace d'alerter le collaborateur sur un risque lié à son propre surf internet que d'organiser une formation cybersécurité. Cela permet de restituer à chaque collaborateur des indicateurs sur la qualité de son comportement et de favoriser ensuite son autorégulation…

3

Donner envie plutôt que d'être anxiogène

Sensibiliser et former sont assurément 2 choses différentes. **Si l'on veut réussir à faire changer les comportements, il faut rapprocher ses actions du contexte et des enjeux de chaque personne**. Les actions de sensibilisation doivent donc rester simples. Certes, le sujet de fond est la présence de l'utilisateur face à un risque mais si l'on cherche à lui faire peur par des communications anxiogènes, on n'atteindra pas les résultats escomptés. Il faut faire preuve de pédagogie et expliquer simplement les choses ou la manière dont procède les cybers criminels par jeux de rôle afin que ce ne soit pas que des contraintes…

Pour donner envie et impliquer plus rapidement les utilisateurs, il ne faut pas hésiter à sortir du cadre professionnel car les cyber menaces ciblent également la dimension personnelle. Quand on sait que de plus en plus de collaborateurs travaillent à distance ou utilisent leurs équipements personnels pour accéder à leur environnement de travail, développer une bonne hygiène informatique à titre personnel améliore également la sécurité de l'organisation. De plus, les exemples de la vie personnelle sont souvent plus percutants et parlants que ceux de l'univers professionnel.

2

Questions à notre expert

Michel Gérard
Président Directeur Général

conscio technologies

Pourquoi faut-il faire de la sensibilisation ?

« Parce que ça marche ! On sait aujourd'hui que 70 à 95% des infections sont liées à des défauts de comportement des utilisateurs. Une étude menée par Aberdeen Group expliquait même que sensibiliser pouvait réduire les incidents liés à la sécurité de l'ordre de 60% ! Aujourd'hui, l'objectif c'est de faire de l'humain un maillon fort car la sécurité ce n'est plus seulement des process, des normes et de la technologie. Si l'on avait mis autant d'énergie et d'argent sur la sensibilisation des personnes que pour les infrastructures, il y aurait bien moins d'attaques réussies aujourd'hui. »

Quel conseil donneriez-vous pour réussir sa campagne de sensibilisation ?

« Lorsque l'on démarre, il est préférable d'organiser une campagne pédagogique qui revienne sur les fondamentaux des bons comportements. On pourra ensuite affiner un dispositif plus organisé de sensibilisation et l'intégrer de manière durable et pérenne à tous les niveaux car c'est une opération de longue haleine. Faire changer les comportements prend du temps, il faut définir une stratégie de sensibilisation qui va s'adapter à chaque niveau d'interlocuteur et qui soit régulière pour engager les utilisateurs. Il faut persévérer si l'on veut obtenir de bons résultats… »

ET DEMAIN ?

Si personne n'a de boule de cristal pour prédire ce que sera le paysage des cyber menaces dans les années à venir, une chose est sûre : vos collaborateurs feront certainement l'objet d'une de ces attaques extrêmement sophistiquées !

La sensibilisation des utilisateurs n'occulte donc pas la nécessité de renforcer les outils informatiques qui composent la chaine de sécurité. D'autant plus que les DSI et RSSI font face aujourd'hui à des perspectives bien sombres en matière de cyber menaces. Les attaques intégrant de l'Intelligence Artificielle vont se développer et permettront aux cybercriminels d'utiliser des modèles d'apprentissage automatique capables de contextualiser leurs faux messages en temps réel avec plus de chances de convaincre leurs cibles…

Mais une chose qui ne changera pas, c'est la nature humaine et les 7 péchés capitaux. Même les utilisateurs les plus avertis sont toujours susceptibles de faire des erreurs à un moment d'inattention. **Sensibiliser les utilisateurs à la cyber sécurité est donc un complément à part entière pour renforcer l'efficacité des outils qui composent la chaîne de sécurité !**

Mais heureusement, les comportements changent et évoluent déjà : les pouvoirs publics s'engagent comme on le constate avec la création de Cybermalveillance.gouv.fr, les éditeurs de logiciels investissent davantage dans la sécurité, les entreprises et collectivités publiques s'organisent…

Il est donc aujourd'hui, indispensable de **relever ce nouveau défi de la cybersécurité pour transformer le facteur humain en maillon fort de sa chaîne de sécurité** grâce à l'organisation régulière de campagnes de sensibilisation innovantes et la mise en place d'outils de sécurité adaptés aux interactions intelligentes avec les utilisateurs finaux.

Olfeo

2 Questions à notre expert

Alexandre Souillé
Président Directeur Général
Olfeo
La sécurité positive

Comment voyez-vous l'avenir en matière de cybersécurité ?

« Il est évident que les attaquants vont eux aussi continuer à monter en compétences et il faut s'attendre à des niveaux de qualité et d'ingénierie sociale très élevés dans les prochains malwares qui feront la une des médias… Sans oublier que l'accélération de la transformation digitale, que ce soit via les services utilisés dans le Cloud, les applications SaaS ou les nouveaux comportements de BYOD et nomadisme, multiplient les points d'interaction numérique avec les utilisateurs qui seront de plus en plus exposés aux cybercriminels. »

Comment les entreprises peuvent-elles s'y préparer ?

« Beaucoup d'entreprises considèrent encore que « ça n'arrive qu'aux autres » alors que faire évoluer les comportements demande du temps et exige de démarrer le plus tôt possible ! Les entreprises doivent prendre conscience qu'elles sont le lieu idéal pour apprendre à mieux réagir face aux cyber menaces, sur le plan personnel et professionnel. Mais une formation n'est pas toujours suffisante pour faire changer les comportements de manière durable, il faut diffuser continuellement des bonnes pratiques et notamment grâce à des interactions intelligentes avec les utilisateurs, intégrées directement dans les outils de protection. »

OLFEO,
LA PASSERELLE DE SÉCURITÉ WEB DISRUPTIVE
BASÉE SUR UNE VISION À 360°.

Olfeo est leader français de la sécurité web.

Nous accompagnons depuis **plus de 16 ans** les **entreprises exigeantes** dans la sécurisation de leur flux web. Grâce à notre **connaissance** extrêmement fine des **besoins des organisations françaises**, nous avons développé une passerelle de sécurité web disruptive, basée sur une **vision globale**, et **pas uniquement technologique**.

Notre passerelle de sécurité web, basée sur une infrastructure Proxy inclut les fonctions suivantes :

- Filtrage web
- Proxy avancé & déchiffrement HTTPS
- Antivirus web
- Filtrage DNS
- Nomadisme
- Campus
- Portail Public
- Filtrage protocolaire

Sensibilisez l'utilisateur final au sein de la solution Olfeo, avec :

- Le coaching, et l'envoi de rapports personnalisés à chaque collaborateur
- La diffusion de la charte informatique auprès de vos équipes
- L'affichage de messages de prévention contextuels lors de navigation web
- Une expérience utilisateur fluide, à juste mesure
- L'envoi de mails contenant des vidéos pédagogiques sur la sécurité

Cet ebook a été créé avec la participation de :

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes de cybermalveillance. Ses publics sont les particuliers, les entreprises et les collectivités (hors OIV). Ses missions portent sur l'assistance aux victimes, l'information et la sensibilisation, et l'observation du risque numérique.

Cybermalveillance.gouv.fr lance un kit de sensibilisation à destination des collaborateurs, composé d'une douzaine d'outils (vidéos, fiches pratiques, infographies...) mis gracieusement à disposition du public en licence ouverte.

https://www.cybermalveillance.gouv.fr/

conscio technologies

Conscio Technologies est le spécialiste de la sensibilisation à la cybersécurité et au RGPD. Conscio Technologies propose une large variété de contenus à base de saynètes, de vidéos et de quiz, ainsi que deux solutions logicielles, Sensiwave et RapidAwareness, permettant aux entreprise de mettre en oeuvre leurs campagnes de sensibilisation. Plus d'un million de personnes ont déjà été sensibilisées au travers des contenus et des solutions de Conscio Technologies.

http://www.conscio-technologies.com/

Olfeo

CONTACTEZ-NOUS

4 rue de Ventadour
75001 Paris
+33(0) 969 390 999

contact@olfeo.com

www.olfeo.com