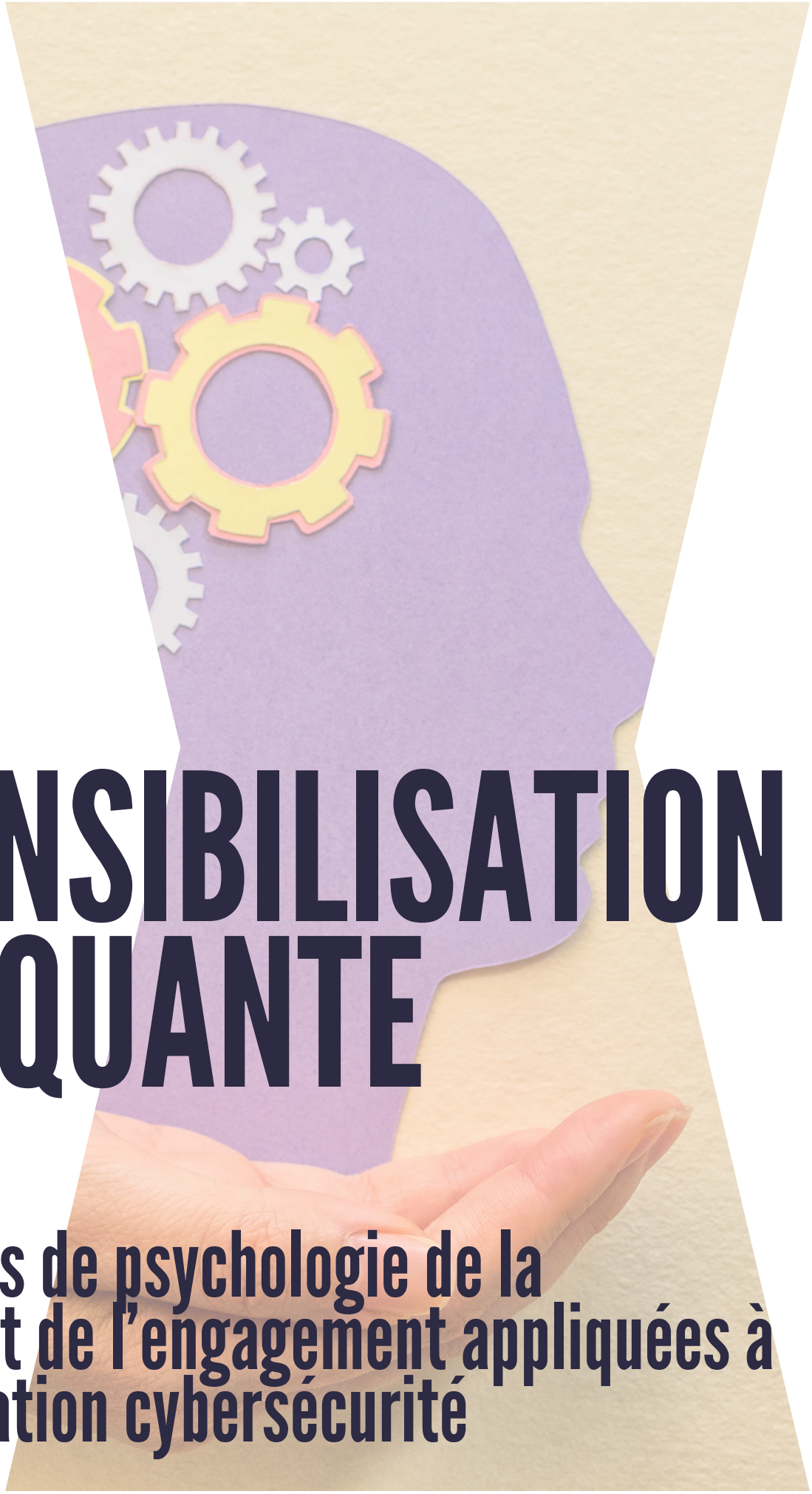


LA SENSIBILISATION IMPLIQUANTE

12 techniques de psychologie de la persuasion et de l'engagement appliquées à la sensibilisation cybersécurité

conscio
Technologies

SOMMAIRE

LE FACTEUR HUMAIN AU COEUR DES ENJEUX DE CYBERSÉCURITÉ

Dans une immense majorité des cas, un **défaut de comportement d'un utilisateur** du système d'information est au **cœur des incidents de sécurité** (60% selon 2022 Ponemon Cost of Insider Threats Global Report, jusque 80% selon d'autres sources).

Le **développement d'une culture cybersécurité** et l'**adoption des bonnes pratiques** par les utilisateurs sont au cœur de toute stratégie cybersécurité.
La plupart des organisations ont ainsi **développé des programmes de sensibilisation des utilisateurs**.

UNE DÉCEPTION

Trop souvent, les organisations sont **déçues des résultats de leurs opérations de sensibilisation**, tant du point de vue de la **participation** que du **résultat sur l'adoption des bonnes pratiques**.

Nombre d'organisations mènent chaque année une campagne annuelle davantage pour des **raisons de conformité que d'amélioration de la sécurité**. Cette approche n'a en effet que **peu d'impact sur les changements de comportements**.

Les employés **ont du mal à retenir et à appliquer** dans leur vie professionnelle quotidienne ce qu'ils ont **appris lors de formations sporadiques**. De plus, la plupart des formations contiennent des **présentations obsolètes**, **banales** et **inintéressantes**, et elles ne sont souvent **pas suffisamment spécifiques aux rôles individuels des employés** au sein de leur organisation.

Cela concorde avec les résultats d'un rapport Usenix sur l'efficacité des formations de sensibilisation au phishing. Les participants ont été invités à identifier les e-mails malveillants à différents intervalles après une formation de sensibilisation à la sécurité, allant d'avant à immédiatement après et quatre, six, huit et 12 mois après. Les **taux de reconnaissance étaient élevés au quatrième mois**, mais les taux de réponse ont **considérablement diminué après six mois**, ce qui suggère que les formations de sensibilisation à la sécurité sont **plus efficaces lorsqu'elles sont organisées deux à trois fois par an**.

DÉMARCHE GÉNÉRALE

Nous travaillons avec les RSSI, DSI et DPO depuis plus de 15 ans, afin de les **aider à développer une réelle culture cybersécurité** au sein de leurs organisations.

Nos équipes n'ont de cesse que de rechercher les **meilleures pratiques et méthodes** favorisant **l'adhésion** et **l'engagement** vers un **comportement cyber sécurisé**.

Nous cherchons ainsi à **guider chaque utilisateur** vers un engagement dans lequel il fait sienne la maxime « ***le piratage informatique ne passera pas par moi*** » et, qu'il ne soit pas une **source d'incidents de sécurité**.

C'est ainsi que nous nous appuyons sur différents travaux de **Robert-Vincent Joule** et de **Fabien Girandola**, tous deux d'Aix Marseille Université, en matière de **psychologie de la persuasion et de l'engagement**.

4 PILIERS

La combinaison de ces travaux nous amène à la mise en œuvre d'une **démarche qui s'appuie sur 4 piliers** :

1. Expliquer les enjeux et développer la sensibilité au sujet :
- En effet, avant toute chose il est indispensable que chacun puisse considérer le sujet comme important.

2. Inculquer un minimum de connaissances :
- Sans chercher l'expertise, la connaissance d'un minimum d'éléments sur le sujet est nécessaire.

3. Savoir se poser les bonnes questions :
- Dans cette étape, nous cherchons à faire en sorte qu'une personne, face aux différentes situations auxquelles elle se trouve confrontée, prenne un temps minimum pour se poser les bonnes questions et y apporter les bonnes réponses.

4. Adopter les nouveaux comportements :
- C'est par la mise en pratique régulière de l'étape 3 qui s'appuie elle-même sur les 2 premières étapes, que de nouveaux réflexes et comportements finissent par être adoptés et deviennent naturels. Des actes engageants viennent renforcer l'adoption des comportements attendus dans la durée.

Joule, R.V. & Beauvois, J.L. (2002). Petit traité de manipulation à l'usage des honnêtes gens. Grenoble : Presses Universitaires de Grenoble.
Joule, R.V. & Beauvois J.L. (1998). La soumission librement consentie. Paris : Presses Universitaires de France.
Girandola, F. (2003). Psychologie de la persuasion et de l'engagement : Presses Universitaires de Franche-Comté.

12 TECHNIQUES D'APPLICATION, DANS UNE STRATÉGIE DE SENSIBILISATION EN LIGNE

D'un point de vue pratique, l'application des travaux de recherche sur la psychologie de la persuasion et de l'engagement nous a conduit à la **mise en œuvre de différentes techniques appliquées** à la **mise en œuvre d'une stratégie de sensibilisation en ligne**.

Ici, nous en présentons **12** qui nous semblent les plus utiles, afin de **maximiser l'impact des opérations de sensibilisation**. D'autres techniques peuvent être imaginées et mises en œuvre, une fois les principes de la psychologie de la persuasion et de l'engagement compris.

1. Du bon usage de la peur
2. Traitement direct du sujet
3. Développement de l'implication
4. Humeur positive
5. Inoculation
6. Casser le sentiment d'invulnérabilité
7. Du bon usage des récompenses
8. Obtenir un acte engageant
9. L'amorçage
10. L'étiquetage
11. L'identification sociale
12. Recadrage

TECHNIQUE N°1
DU BON USAGE DE LA PEUR

La **peur** est **très souvent utilisée** quand il s'agit de **cybersécurité**. On mettra ainsi en avant les **profils menaçants des pirates** et des **organisations criminelles** qui les utilisent, les **conséquences désastreuses des attaques** sur les **organisations** et sur les **collaborateurs** qui en sont victimes.

La **recherche** montre que lorsqu'on **utilise la peur pour persuader une personne** du bienfondé du comportement qu'on lui demande, on peut provoquer **deux types de réactions** : la **gestion de la peur** ou la **gestion du danger**.

La première réaction est **contreproductive**. Il s'agit d'**éviter le problème en le contournant** de façon à **dénier ou minimiser le sujet**, et en **transférant la responsabilité** sur un tiers ou tout simplement en **faisant preuve de fatalisme**.

La deuxième réaction correspond à ce qu'on **cherche à obtenir**, à savoir la **mise en œuvre des bonnes pratiques**, permettant d'éviter que **la menace se concrétise**.

Ici aussi, la recherche montre qu'on obtient cette deuxième réaction à condition d'expliquer en même temps, l'intention de **susciter la peur**, les **mesures à prendre** pour faire face au danger, leur **efficacité** et leur **simplicité** de mise en œuvre.

En matière de sensibilisation à la cybersécurité, il faut ainsi au même moment qu'on met en avant la menace, les risques et les conséquences des incidents, **expliquer aux utilisateurs que l'application de quelques règles et comportements simples permettront de les éviter**.

En conclusion les appels à la peur sont particulièrement efficaces quand :

Ils décrivent une menace en **accentuant la sévérité et la vulnérabilité**

Ils font état de **l'efficacité des recommandations et de leur facilité d'exécution**

TECHNIQUE N°2
TRAITEMENT DIRECT DU SUJET

Le message délivré a **tendance à convaincre davantage sans avertissement préalable**.

En étant averti avant, il existe une **tendance à imaginer les résistances**.

Même si ce phénomène est moins marqué sur les sujets techniques ou l'avertissement (à moins d'impact négatif), il peut être intéressant d'**apporter directement l'information sans annonce**.

Cela peut être le cas de **campagnes très ciblées** dans lesquelles le message d'invitation commence à **traiter directement du sujet choisi** et **propose de suivre immédiatement le support proposé**. Il peut aussi présenter un risque et les dangers associés tout en proposant de suivre le support qui donne simplement les moyens de s'en protéger.

Cela peut également se retrouver dans **l'envoi de messages de sensibilisation** dans le **flux d'une messagerie instantanée** de type Slack, WhatsApp ou Teams.

TECHNIQUE N°3 DÉVELOPPEMENT DE L'IMPLICATION

Plus le sujet sera perçu comme **important**, plus les utilisateurs auront tendance à se **sentir impliqués**. Cela peut se traduire notamment par une **communication appropriée** mettant en avant le fait que le sujet soit **essentiel pour l'organisation** et l'**alignement** de la direction et tout le management **pour en faire une priorité**.

L'implication sera également d'autant plus forte que les situations présentées colleront **au plus près du vécu des utilisateurs**. C'est pourquoi Conscio Technologies, **en collaboration avec ses clients**, a créé des **contenus sectoriels** (santé, collectivités territoriales, industrie et retail). De plus, l'utilisation des **fonctions de personnalisation** de la solution Sensiwave, permet à chaque client d'**adapter les contenus** pour coller au mieux à l'environnement de leurs collaborateurs.

TECHNIQUE N°4
HUMEUR POSITIVE

Il est démontré que les **individus de bonne humeur** désirent **perdurer cet état** et donc traitent le message s'il permet de **maintenir cette humeur positive**.

On cherchera donc à **diffuser des supports plaisants** voire **ludiques** ou faisant preuve **d'humour** qui favoriseront cette humeur positive.

C'est ce que l'on retrouve dans les **supports de sensibilisation proposés par Conscio Technologies** (vidéos Funny but Serious, Cyberhéros, vidéos interactives, bandes dessinées interactives...).

Un collaborateur de bonne humeur est plus **réceptif aux messages**.

Idée : intégrez de l'humour ou des éléments ludiques dans vos supports.

TECHNIQUE N°5
INOCULATION

Il s'agit ici de **lutter de façon préventive** contre les **freins** et **résistances**. L'inoculation consiste à présenter la **tentation**, une ou plusieurs **résistances** et son **contre argumentaire**. Cela a pour effet d'**élaborer un schéma de réponse** lorsque la tentation réelle se présentera.

Anticipez les objections potentielles en exposant des arguments contraires, puis en les déconstruisant.

Exemple : « Beaucoup pensent que seuls les grandes entreprises sont ciblées, mais voici pourquoi toute organisation est une cible : ... »

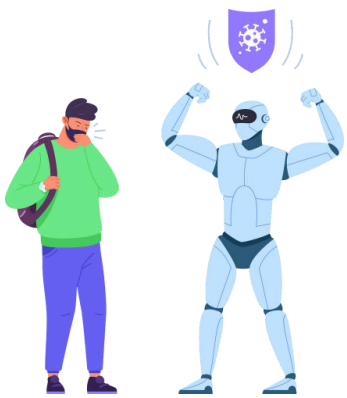
TECHNIQUE N°6
CASSER LE SENTIMENT D'INVULNÉRABILITÉ

Il peut en effet y avoir dans une partie des collaborateurs, une sorte de **sentiment d'invulnérabilité**.
Cela peut se traduire par des réactions du type « **ce n'est pas moi qui me ferais avoir** » ou « **dans notre entreprise l'équipe technique est très forte, elle arrivera à empêcher que ça se produise** » ou encore « **nous ne sommes pas une cible, ça ne risque pas de nous arriver** ».
On peut bien sûr imaginer toutes sortes de variantes à ces réactions.

On s'attachera donc à mettre en avant des cas d'incidents survenus dans des organisations similaires.

Des opérations de tests phishings pourront également montrer que tout le monde peut se faire avoir.

Certains collaborateurs pensent **ne jamais être victimes d'une attaque**. Montrez-leur que **personne n'est à l'abri**.



TECHNIQUE N°7
DU BON USAGE DES RÉCOMPENSES

L'idée ici est que **le moins possible est le mieux**.

En effet la recherche a montré que plus la **récompense** ou la **punition est forte**, plus **l'engagement est faible**. En effet, les **raisons d'ordre interne resserrent les liens** entre l'individu et ses actes alors qu'une **raison externe** telle que la récompense, non.

Il peut cependant être tentant d'**associer des cadeaux aux opérations de sensibilisation** afin d'en **favoriser la participation**. Il faut dans ce cas en garder le **caractère symbolique** et ne le faire que dans le cadre d'un **événement bien délimité sans le systématiser**.

Des récompenses **trop importantes diminuent l'engagement** personnel des collaborateurs.

Idée : proposez un badge virtuel ou une mention spéciale.

TECHNIQUE N°8
OBTENIR UN ACTE ENGAGEANT

Retenons simplement que le but est d'**obtenir un comportement initial engageant l'utilisateur vers l'adoption des bonnes pratiques souhaitées**.

Les **caractéristiques de l'acte** permettant un **fort engagement** sont :

Le contexte de **liberté** dans lequel l'acte est réalisé

Le **caractère public** de l'acte

Le **caractère explicite** de l'acte

L'irrévocabilité de l'acte

La **répétition** de l'acte

Les **conséquences** de l'acte

Le **coût** de l'acte

Les **raisons** de l'acte

TECHNIQUE N°8
OBTENIR UN ACTE ENGAGEANT
(SUITE)

Nous n'entrerons pas ici dans le détail de la théorie de la psychologie de l'engagement. On peut également se **reporter aux ouvrages de Robert Vincent Joule ou de Fabien Girandola**.

Retenons simplement que le but est d'**obtenir un comportement initial engageant l'utilisateur vers l'adoption des bonnes pratiques souhaitées**.

Les **caractéristiques de l'acte** permettant un **fort engagement** sont :

Le contexte de liberté dans lequel l'acte est réalisé : un acte réalisé dans un contexte de liberté est plus engageant qu'un acte réalisé dans un contexte de contrainte.

Le caractère public de l'acte : un acte réalisé publiquement est plus engageant qu'un acte dont l'anonymat est garanti.

Le caractère explicite de l'acte : un acte explicite est plus engageant qu'un acte ambigu.

L'irrévocabilité de l'acte : un acte irrévocable est plus engageant qu'un acte qui ne l'est pas.

La répétition de l'acte : un acte que l'on répète est plus engageant qu'un acte qu'on ne réalise qu'une fois.

Les conséquences de l'acte : un acte est d'autant plus engageant qu'il est lourd de conséquences.

Le coût de l'acte : un acte est d'autant plus engageant qu'il est coûteux (en argent, en temps, en énergie, etc.).

Les raisons de l'acte : un acte est d'autant plus engageant qu'il ne peut être imputé à des raisons externes (par exemple : promesses de récompenses, menaces de punition) et qu'il peut être imputé des raisons internes (par exemple : valeurs personnelles, traits de personnalité).

TECHNIQUE N°8
OBTENIR UN ACTE ENGAGEANT
(SUITE)

Nous donnons ici **deux exemples d'actes engageants** pouvant être utilisés dans les **parcours de sensibilisation en ligne** :

MACARON

Conscio Technologies propose le macaron « **Le piratage informatique ne passera pas par moi** ».

Celui-ci peut être adapté pour correspondre aux critères graphiques du client.

Pour l'obtenir, voici la procédure :

1. Dans un premier **quiz**, il est simplement demandé à la personne si elle est d'accord pour dire : que la **cybersécurité** est l'un des **principaux enjeux de la décennie** et, qu'elle est d'accord de dire que dans ce domaine, **chacun a un rôle à jouer**,
2. À la suite d'une réponse favorable, on lui propose de **faire partie de cet élan général** et **d'afficher son adhésion** par le téléchargement du **macaron** qu'elle pourra **déployer sur ses réseaux sociaux** (LinkedIn, etc...) ainsi que sur **celui de l'organisation**, s'il existe,
3. On la **remercie** de son engagement pour un **monde cyber plus sûr**, en précisant qu'ainsi il se pourrait qu'elle **fasse la différence**.

DEMANDE DE RÉPONSE

Moins coûteux que le comportement demandé d'afficher le macaron, il s'agit ici d'**agrémenter les différents parcours de demandes d'engagement**.

Par exemple, à l'issue d'un module de sensibilisation, on peut afficher une affirmation comme « **J'ai bien compris que le succès de notre cybersécurité dépend de l'effort de chacun, et je m'engage moi aussi à ce que le piratage informatique ne passe pas par moi** », suivie par un choix **oui/non**, sur lequel clique la personne.

Moins couteux, moins public que le premier acte proposé, il n'en reste pas moins **engageant** dans le sens où la personne sait que **ses réponses sont enregistrées**.

TECHNIQUE N°9
L'AMORÇAGE

Il s'agit ici de faire en sorte que la personne **amorce une adoption des comportements demandés**.

Une bonne façon de l'appliquer : dans le cas où l'on recense x règles de sécurité à suivre, s'adresser à l'utilisateur de la façon suivante : « **Nous comprenons bien qu'appliquer les x règles de sécurité dès maintenant dans leur ensemble peut s'avérer compliqué. Ce que nous vous demandons en fait aujourd'hui, est de choisir une de ces règles parmi les x, celle que vous voulez et de vous engager à la respecter dès maintenant** ».

Il se produit alors en général la chose suivante :

Les personnes considèrent que **l'effort demandé n'est pas si grand**, ils ont la liberté de **choisir** la règle qu'ils veulent.

Ils ont donc tendance à effectivement **respecter** la règle qu'ils ont choisie.

Par effet de halo, lorsqu'ils sont confrontés à des situations impliquant les autres règles, ils ont également **tendance à les suivre**.

TECHNIQUE N°10
L'ÉTIQUETAGE

Il s'agit de **valoriser en la qualifiant**, la personne qui effectue une campagne de sensibilisation ou s'engage d'une façon ou d'une autre.

On ne se contente pas de la remercier, on y ajoute une **mention la qualifiant**.

Par exemple : « **Nous vous remercions d'avoir terminé cette campagne de sensibilisation. Cela montre que vous êtes responsable et faites partie des personnes qui rendent le monde cyber plus sûr** ».

Valorisez publiquement les collaborateurs engagés pour renforcer leur motivation.

TECHNIQUE N°11
L'IDENTIFICATION SOCIALE

L'engagement d'une personne se trouvera **renforcé** si elle a le sentiment de ne pas être un cas isolé et de participer à un élan général.

Pour ce faire, on pourra donner des **éléments statistiques sur le développement de la stratégie de sensibilisation** et des **éléments plus qualitatifs de retour d'expérience** ou d'**avis d'autres collaborateurs**.

Les utilisateurs s'engagent davantage s'ils se sentent appartenir à un groupe partageant les mêmes objectifs.

Conseil : partagez des statistiques sur l'engagement collectif, comme « 80 % de vos collègues ont suivi cette formation. »

TECHNIQUE N°12
RECADRAGE

Il s'agit d'éclairer le contexte d'une façon nouvelle, afin d'**amener la personne à adapter son modèle de représentation vers une vision plus positive**.

Par exemple, cela peut dans notre cas passer par l'**interpellation de l'utilisateur** à un moment opportun du parcours par une phrase du genre : **Acceptez-vous de vous engager pour un monde cyber plus sûr ? Vous pourriez faire la différence !**

Proposez une nouvelle manière de voir la cybersécurité pour motiver les utilisateurs à s'impliquer.

Exemple : « Vous contribuez vous aussi à rendre notre service plus sûr » .

TÉLÉPHONE : 01 84 80 82 00

MAIL : contact@conscio-technologies.com

SITE : www.conscio-technologies.com

ADRESSE : 3 rue Camille Claudel, 56890 PLESCOP

conscio
Technologies