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… »