sosafe

Sécurité comportementale

Mieux sensibiliser grâce aux mesures comportementales

Table des matières

01 Introduction

Le pouvoir des sciences comportementales au service de la cybersécurité

Personne ne dira le contraire : la sécurité des données est, pour les entreprises, l'un des défis les plus pressants de notre époque. Les cyberattaques ne se font pas seulement plus fréquentes : elles ont aussi gagné en subtilité. De nombreux criminels ont, en effet, compris le pouvoir de l'ingénierie sociale, de sorte que leurs pièges sont difficiles à repérer, et plus encore à éviter.

Il faut dire que les tactiques d'ingénierie sociale qu'ils utilisent pour manipuler leurs victimes sont étroitement liées aux schémas comportementaux humains. Pour contre-attaquer, les mesures destinées à assurer la protection des entreprises doivent donc adopter une approche similaire. La dynamique qui caractérise aujourd'hui le paysage des menaces a poussé de nombreux professionnels de la sécurité à repenser leurs stratégies défensives pour passer de mesures purement techniques à une approche plus holistique qui place l'humain au centre du dispositif de cybersécurité. Désormais, l'une des priorités, pour ne pas dire la priorité, dans le développement d'une solide culture de la sécurité, est de « faire évoluer les comportements ». Il s'agit d'inciter les collaborateurs à réfléchir à leurs actions et à instaurer des routines défensives qui laissent peu de chances aux cybercriminels de parvenir à leurs fins.

C'est en cherchant à mieux comprendre les rouages qui sous-tendent les comportements des attaquants comme ceux des utilisateurs, et l'impact que peuvent avoir certaines mesures sur l'attitude de ces derniers, que les entreprises auront tout en main pour anticiper les attaques et les neutraliser en amont. Des mesures comportementales précises et pertinentes ne sont pas uniquement des outils mis à la disposition des décisionnaires pour les aider à comprendre les réactions de leurs employés face aux différentes sortes de menaces. Elles leur permettent également de déterminer quel type de formation leur sera particulièrement profitable et d'ajuster constamment les actions de sensibilisation en fonction des progrès des utilisateurs. Par exemple, si le taux d'alerte phishing est moins fort dans une équipe que dans les autres, il suffira peut-être de quelques rappels sur la formation en ligne pour amener ces collaborateurs à mieux identifier et signaler les e-mails suspects. Enfin, les mesures comportementales donnent une idée claire des effets qu'a le programme de sensibilisation sur la culture et la sécurité globale de l'entreprise. Ces chiffres sont souvent très parlants pour les différents intervenants, que ce soit la direction ou les employés.

Deux questions se posent :

Sur quelles mesures une entreprise doit-elle se concentrer lorsqu'elle souhaite évaluer l'efficacité des actions mises en place pour développer sa culture de la cybersécurité ?

Et quelles sont **les méthodes inspirées des sciences comportementales** qui permettent de renforcer l'impact de la sensibilisation à la sécurité ?

Pour y répondre, nous allons, dans un premier temps, nous pencher sur les relations entre les sciences comportementales et la cybersécurité. Nous détaillerons ensuite les différentes facettes à prendre en compte pour établir une culture holistique de la sécurité, ainsi que les mesures utiles pour déterminer l'efficacité des actions mises en place.

02 Qu'est-ce qui pousse les entreprises à mesurer l'évolution des comportements en matière de cybersécurité ?

C'est aujourd'hui une évidence pour les spécialistes de la cybersécurité : la technologie seule ne suffit plus pour protéger les entreprises des attaques, de plus en plus sophistiquées, des cybercriminels. L'ingénierie sociale est devenue leur arme de prédilection depuis qu'ils ont compris qu'en jouant sur le facteur humain, ils augmentaient, de façon indécente, leurs chances de réussir. **En effet, selon le dernier rapport « Data Breach Investigations Report » de Verizon, plus de 82 % des violations de données impliquent un élément humain.**[1] Dans le même ordre d'idées, IBM classe les vols d'identifiants et l'hameçonnage – deux types de compromissions étroitement liées au facteur humain – comme les deux principaux vecteurs d'attaque. [2]

Les sociétés payent le prix fort face aux capacités d'innovation des criminels

Ces nouvelles tendances qui redessinent le paysage des menaces cyber ont eu de lourdes conséquences financières sur les sociétés du monde entier, notamment pour de grands noms tels que Twilio, Cisco et Uber. Ces trois entreprises ont récemment fait la triste expérience du danger que représente l'ingénierie sociale.

Twilio a, en effet, déclaré avoir eu connaissance « d'un accès non autorisé à des informations liées à un nombre limité [plus de 120] de comptes clients de Twilio par le biais d'une attaque sophistiquée » ayant réussi à piéger certains de ces employés. Les criminels avaient envoyé des SMS de phishing personnalisés (« smishing ») aux collaborateurs pour les amener à divulguer des données sensibles.[3]

Le prestataire en « Threat intelligence » Cisco Talos a lui aussi annoncé au public que près de 3 Go de données lui avaient été dérobés lors d'une attaque liée au gang du rançongiciel Yanluowang.[4] Les attaquants ont réussi à détourner le compte personnel Google d'un collaborateur de Cisco sur lequel étaient enregistrés des identifiants de connexion sensibles. Ils ont ensuite utilisé la technique du phishing vocal ou « vishing » pour pousser les employés à accepter des

1 Verizon (2022). Data Breach Investigations Report.
2 IBM (2022). Cost of a Data Breach Report.
3 Twilio (2022). Incident Report: Employee and Customer Account Compromise.
4 LeMagIT (2022). Cyberattaque : comment Cisco a repoussé Yanluowang.

processus MFA et infiltrer ainsi les systèmes internes de la société.

Mais l'attaque d'ingénierie sociale la plus marquante de toutes est probablement celle qui a frappé Uber, le géant des services de transport, en septembre 2022.[5] On pense qu'elle est l'œuvre d'un jeune hacker de 18 ans qui aurait contourné un processus MFA vulnérable et utilisé la technique de l'homme du milieu pour pousser un utilisateur à communiquer, sans le savoir, ses identifiants de connexion. Le pirate a alors eu accès à l'environnement interne d'Uber où se trouvent les bases de données et les plateformes de communication.

Le télétravail et les progrès de la technologie augmentent le risque de cyberattaques

En réalité, les capacités d'innovation et les nouvelles tactiques des cybercriminels ne constituent qu'une partie du problème. Bien d'autres facteurs viennent s'y ajouter, confirmant la tendance actuelle qui est de cibler le facteur humain. Ces deux dernières années, de multiples formes de télétravail se sont développées autour de nouveaux processus et outils collaboratifs. Or, ces outils sont aussi la porte ouverte à de nouvelles attaques, non seulement parce qu'ils offrent de nouveaux points d'entrée potentiels dans les systèmes des sociétés, mais aussi parce que leur prise en main présuppose une période de transition pendant laquelle les employés, moins sûrs d'eux, se laissent plus facilement duper. Dans le même temps, les progrès de la technologie mettent en péril la sécurité des informations de manière plus générale. Il ne faut pas sous-estimer, à cet égard, le pouvoir de l'intelligence artificielle (IA). Les techniques, telles que le clonage vocal qui permet d'imiter la voix d'une personne en vue d'une utilisation malveillante, sont de plus en plus faciles à manipuler. Avec l'IA as-a-service, ces nouveaux outils pourraient même bientôt se trouver à la portée des non-initiés et donner un nouvel élan aux méthodes d'attaques actuelles comme le spear phishing.

Une question essentielle se pose : comment se protéger de ces menaces ?

Alors que la sensibilisation à la cybersécurité joue, depuis longtemps déjà, un rôle majeur dans le système de défense des sociétés et industries de toute taille, nous assistons aujourd'hui à un changement de paradigme. Les anciens modèles de formation, qui consistaient simplement à s'acquitter des obligations réglementaires et à compulser des bibliothèques de contenus statiques, ne sont plus assez efficaces pour protéger les entreprises face aux dernières innovations d'une cybercriminalité qui se professionnalise. Il faut désormais une culture plus mature de la sécurité avec une approche de sensibilisation holistique. Il ne s'agit plus de viser uniquement la conformité aux règlements, mais de développer, chez les employés, des réflexes de sécurité qui leur permettent d'effectuer leur travail quotidien sans se mettre en danger. Ainsi, en intégrant les principes des sciences comportementales dans leurs programmes de sensibilisation à la cybersécurité, les entreprises pourront passer de mesures ponctuelles à l'instauration d'une culture durable de la sécurité faisant efficacement barrage aux tentatives d'ingénierie sociale.

[5] Ars Technica (2022). Uber was breached to its core, purportedly by an 18-year-old. Here's what's known.

Quantifier l'évolution des comportements : quels avantages ?

Pour parvenir à ce stade, il est indispensable de s'appuyer sur des chiffres pertinents qui illustrent la progression de cette culture de la sécurité et les changements qui s'opèrent dans les habitudes des collaborateurs. Ces mesures comportementales sont des outils très efficaces que les RSSI et les professionnels de la cybersécurité utilisent au quotidien. **Intégrées aux stratégies de défense et de signalement, elles présentent plusieurs avantages :**

Elles aident à définir les schémas comportementaux typiques des collaborateurs, en cas d'attaque par exemple. Comment réagissent-ils ? À quels types d'attaque sont-ils plus vulnérables ? Quels éléments favorisent ou, au contraire, freinent leur processus d'apprentissage ?

Elles permettent aux décisionnaires de combler les lacunes ainsi mises à jour et de renforcer leur système de défense en conséquence. Les collaborateurs ont-ils besoin de facteurs motivants pour mener à bien leur formation ? Quels sujets ont-ils besoin d'approfondir davantage ?

Elles servent d'arguments tangibles dans les échanges avec les différents intervenants que ce soit auprès de la direction ou des employés, afin de présenter l'impact positif des réflexes de sécurité sur la protection de l'entreprise dans son ensemble. Elles peuvent même être mises en relation avec des objectifs que la société a atteints sur le plan financier. Dans quelle mesure le programme de sensibilisation a-t-il favorisé l'émergence de comportements plus vigilants ? A-t-il aidé à limiter les risques d'attaques susceptibles de coûter cher à l'entreprise, par exemple ?

Déterminer les mesures pertinentes pour votre entreprise

Il n'y a pas de réponse toute faite ou universelle lorsqu'il s'agit de définir avec précision les mesures comportementales qu'une entreprise doit surveiller. Dans chaque société, les professionnels seront amenés à accorder plus d'attention aux ICP qui correspondent à leurs besoins et à leur contexte, notamment à leur secteur d'activité. Ces mesures comportementales peuvent aller bien au-delà d'un simple taux de signalement ou d'un pourcentage de personnes ayant terminé la formation. Outre les données recueillies pendant la sensibilisation, elles peuvent aussi prendre en compte les comportements des utilisateurs en ligne : ont-ils recours un gestionnaire de mots de passe ? Ont-ils accepté les politiques internes ? Attendent-ils l'approbation du service informatique avant de télécharger une application ? Enfin, des mesures comportementales sophistiquées permettront d'évaluer plus précisément le risque cyber, un ICP plutôt complexe. Les entreprises auront ainsi toutes les clés en main pour activer des mécanismes de défense proactifs aux points stratégiques.

LE SAVIEZ-VOUS ?

Superposer les évaluations traditionnelles avec les mesures comportementales de nouvelle génération

Dans un contexte en constante évolution, les entreprises ont tout intérêt à ne pas tout miser sur les paramètres « traditionnels » axés essentiellement sur la performance (tels que le taux de clics), mais à y associer des mesures comportementales qui donnent davantage une vue d'ensemble (par exemple, le taux d'alerte phishing). Superposées, ces valeurs révéleront rapidement l'impact des mesures de sensibilisation sur les comportements qui caractérisent la culture de sécurité de l'entreprise.

Voici quelques exemples de ces différents paramètres :

Mesures de sensibilisation traditionnelles	Mesures comportementales de nouvelle génération
Taux de clics lors des simulations de phishing	Taux d'alerte phishing à l'aide des outils de signalement intégrés
Taux d'ouverture des e-mails lors des simulations de phishing	Taux d'interaction avec les e-mails et les pages des simulations de phishing
Pourcentage d'utilisateurs ayant suivi une formation sur la sécurité des mots de passe	Taux d'utilisation quotidienne ou hebdomadaire d'un gestionnaire de mots de passe
Pourcentage d'utilisateurs ayant suivi une formation sur la confidentialité des données	Nombre d'actifs de données correctement identifiés avec leur statut de confidentialité sur l'Intranet de la société
Pourcentage d'utilisateurs ayant visionné une vidéo sur le shadow IT	Nombre de demandes d'approbation de logiciel envoyées au service informatique

Comme nous l'avons expliqué plus haut, l'intégration des sciences comportementales dans une stratégie de défense est moins simple qu'il n'y paraît et les directives varient d'une entreprise à l'autre. Nous allons donc nous pencher sur les caractéristiques d'une culture mature de la sécurité, ainsi que sur certaines des mesures comportementales et méthodes pouvant être mises en œuvre pour y parvenir, au sein des entreprises.

03 Le modèle de sécurité comportementale

Construire une culture de la sécurité qui place l'humain au centre

L'évolution constante des menaces cyber rend la situation de plus en plus complexe. Or, le point commun de la plupart des cyberattaques est, incontestablement, le facteur humain. Les entreprises ont beau prendre toutes les précautions nécessaires sur le plan technologique, elles restent vulnérables tant qu'elles n'ont pas compris que leurs employés sont un élément clé de la solution. Alors que les pertes liées à la cybercriminalité se chiffrent aujourd'hui à plusieurs milliers de dollars, il devient impératif, pour les entreprises, de former leurs ressources humaines à la cybersécurité de façon à se protéger efficacement sur le long terme.

Le **« modèle de sécurité comportementale »** met l'accent sur les principaux aspects de cette approche axée sur l'humain. Chacun d'eux contribue à l'objectif final : développer une culture de la sécurité qui protège vraiment. Au lieu de les regarder comme des éléments secondaires, il s'agit de les considérer comme des moteurs comportementaux. Chacun de ces éléments entraîne les autres tout en renforçant les capacités d'auto-défense numérique de l'entreprise. Recueillez toutes les mesures qui vous permettront de définir le degré de maturité de votre culture de la sécurité, dans chacune de ces dimensions. Vous serez alors en mesure d'identifier les risques auxquels votre société est exposée et d'y remédier de manière proactive.

3.1 Savoir : apporter des connaissances et des bonnes pratiques qui restent ancrées dans les esprits

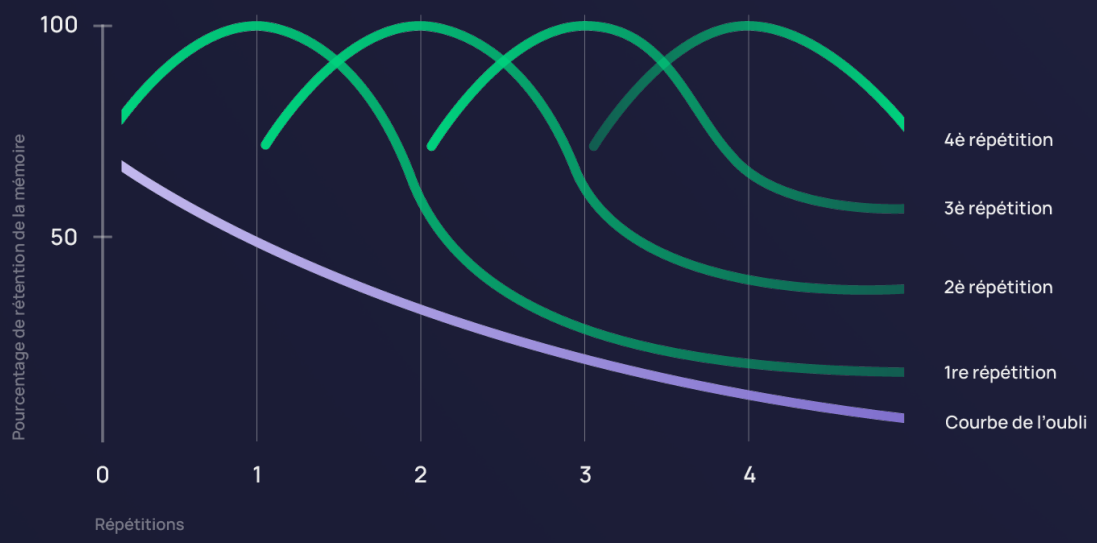
Une formation lacunaire et qui n'est pas axée sur l'humain peut involontairement laisser la porte ouverte à une certaine négligence sur le plan de la cybersécurité. Des collaborateurs qui ne se sentent pas impliqués ne verront pas la nécessité d'être proactifs et réactifs aux cyberattaques. Ils mettent alors en péril à la fois leur propre sécurité et celle de la société. Tout le monde est perdant. Les programmes de sensibilisation à la sécurité devraient être conçus pour attirer l'attention des employés sur le rôle qu'ils ont à jouer en identifiant et en signalant d'éventuelles attaques. Pour que les collaborateurs puissent adopter un certain nombre de réflexes défensifs, il faut les équiper en leur transmettant un savoir sur les meilleures pratiques en matière de sécurité.

Si vous devez augmenter les connaissances de vos collaborateurs, c'est principalement parce que les hackers, eux, ne cessent jamais d'apprendre. D'où l'importance de mettre en place, au sein des entreprises, une formation continue. Autrefois, la transmission des connaissances se faisait souvent de manière linéaire et à fortes doses. Pourtant, nous savons tous que les ateliers interminables et les sessions monotones de formation ne sont pas seulement dépassés. Ils n'atteignent tout simplement pas leur objectif qui est d'ancrer littéralement ce savoir dans les mémoires. La raison en est simple : on sait que, naturellement, la rétention des connaissances décline de manière exponentielle. Le défi est donc de taille, lorsqu'il s'agit d'apprendre et de progresser.

La courbe de l'oubli d'Ebbinghaus [6] montre que, dans un contexte de formation, les apprenants peuvent oublier, dans les 7 premiers jours, 90 % de ce qu'ils ont appris. Cette déperdition augmente encore lorsque les utilisateurs interrompent leurs schémas d'apprentissage ou la fréquence des rappels. Il existe pourtant des méthodes pour améliorer la mémorisation et conserver ainsi le bénéfice de la formation. La répétition espacée consiste à revenir régulièrement sur les informations, par le biais de différents canaux, pour permettre aux utilisateurs de se rappeler ce qu'ils ont appris. Combinée à des éléments interactifs et incitatifs comme des quiz, cette stratégie est particulièrement efficace pour contrer la courbe de l'oubli.

RÉPÉTITION ESPACÉE

Exemple de courbe d'apprentissage favorisant la rétention des informations



6 Growth Engineering (2020). What is the forgetting curve?

> « Les rappels automatisés réguliers augmentent le taux d'engagement de 30 %, parfois même jusqu'à 90 % pendant la phase de lancement. »

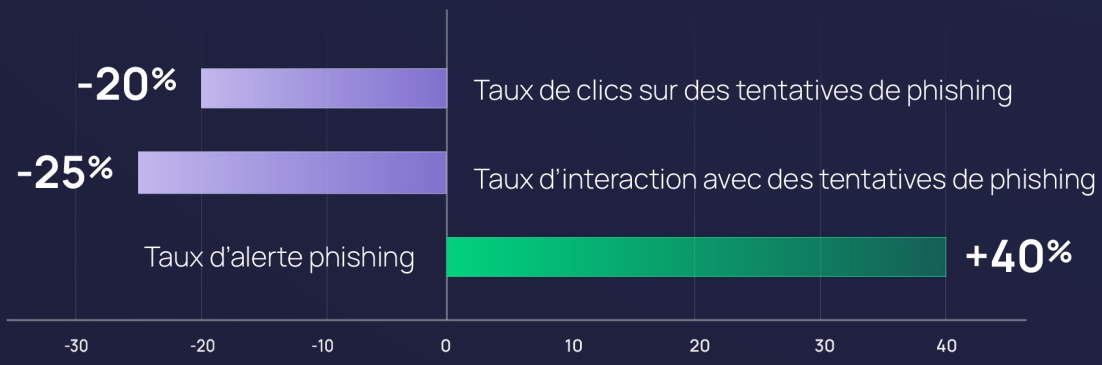
Parmi les méthodes de répétition espacée garantissant un apprentissage plus durable, les rappels automatisés sont particulièrement efficaces. Comme précisé dans notre dernier rapport Human Risk Review : « Les rappels automatisés réguliers augmentent le taux d'engagement de 30 %, parfois même jusqu'à 90 % pendant la phase de lancement. »[7] Les rappels, qui peuvent prendre par exemple la forme d'e-mails réguliers envoyés automatiquement par le système, alimentent le côté interactif et stimulent la vigilance. Ils peuvent être formulés comme des encouragements, des pense-bêtes ou des informations sur la progression, par exemple. L'objectif est de veiller à ce que les utilisateurs restent constants dans leurs efforts.

Les chiffres prouvent, de manière impressionnante, que la consolidation des connaissances, par des méthodes telles que la répétition espacée et les rappels systématiques, est essentielle pour développer une solide culture de la sécurité. Ainsi, les personnes ayant terminé les modules d'apprentissage sur la cybersécurité et la protection des données sont plus perspicaces lorsqu'il s'agit de démasquer les e-mails malveillants et de prévenir les tentatives de phishing. Les données recueillies sur la plateforme SoSafe montrent également que ces employés sont 40 % plus susceptibles de signaler les tentatives de phishing que ceux qui n'ont pas terminé le module de formation.

De manière générale, les employés qui ont bien saisi les rouages de l'auto-défense numérique et disposent de solides connaissances sont des atouts pour aider les entreprises à limiter les risques d'incidents. Un programme de formation bien pensé, avec un apport continu de connaissances contextualisées, est un outil efficace pour y parvenir.

UTILISATION DU PRODUIT

Résultats provenant des utilisateurs avec des taux élevés d'achèvement des modules



Exemples de mesures comportementales permettant de dresser un état des lieux des connaissances :

- → Pourcentage de personnes ayant terminé la formation en ligne
- → Impact des rappels automatisés sur le taux d'engagement
- → Impact du pourcentage d'achèvement de la formation en ligne sur les taux d'alerte phishing

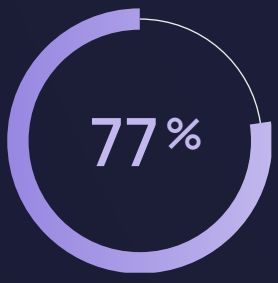
[7] SoSafe (2022). Human Risk Review 2022.

3.2 Contexte : une formation cohérente avec les facteurs de risque propres à l'entreprise

S'il y a un facteur prouvant qu'il n'existe pas d'approche unique et universelle en matière de formation à la cybersécurité, c'est bien le contexte. Opter pour un programme de sensibilisation standardisé, qui mettrait tous les apprenants au même niveau, ce serait faire fi des différences inhérentes à l'entreprise. De toute évidence, les directeurs exécutifs ou les employés possédant un téléphone de fonction sont davantage exposés que des stagiaires, par exemple.

Par conséquent, les cybercriminels ne tendront probablement pas les mêmes pièges aux différents niveaux de hiérarchie dans votre entreprise. Loin de nous l'idée de suggérer que certaines personnes ne sont pas concernées par la menace cyber. Tout le monde est concerné. Mais il faut accorder à chaque niveau de risque l'attention qu'il requiert tout en maintenant une stratégie de réponse cohérente. Il est donc important de bien étudier les rôles et les responsabilités de chaque collaborateur, et de connaître les risques auxquels les uns et les autres sont exposés. Dans la mesure où les dangers varient d'un employé à l'autre, il est essentiel de personnaliser la formation en conséquence.

Avec de tels parcours personnalisés, la formation sera plus concrète, plus en phase avec la réalité et donc plus efficace pour limiter les risques cyber. Selon une enquête menée par Towards Maturity, 77 % d'apprenants souhaitent avoir accès à du contenu qui leur soit utile dans leur travail. [8] Une approche comportementale se concentre sur les collaborateurs, avec les défis qui leur sont propres, et leur propose du contenu en rapport avec leur fonction, leur profil et leur degré de sensibilisation.



des actifs pensent qu'une formation doit leur permettre de mieux faire leur métier.

8 Towards Maturity (2017). Modern learning content for modern workers.

Le secteur d'activité d'une société joue également un rôle majeur dans le niveau de risques auxquels elle est exposée. Les domaines de la santé, les banques et le secteur public comptent parmi les cibles privilégiées des cybercriminels. Il peut donc être essentiel, pour aiguiser la vigilance des employés, de publier des politiques internes spécifiques. Plus les connaissances transmises sont contextualisées, mieux elles sont retenues par le personnel.

La question du contexte se pose aussi sous un autre angle : les entreprises ne doivent pas seulement proposer des formations personnalisées, mais aussi créer un contexte qui encourage les comportements sécurisés. Il s'agit d'incorporer, dans l'infrastructure existante, des composants et des outils qui permettent aux employés de prendre une part active à la stratégie de défense. La tâche est plus facile si l'on dispose d'une plateforme de sensibilisation avec des fonctionnalités intégrées qui simplifient la détection et le signalement des activités suspectes. Les statistiques montrent, par exemple, que le bouton d'alerte phishing de SoSafe permet de réduire de 30 % les interactions des collaborateurs avec les e-mails de phishing. Cette fonctionnalité contextuelle limite ainsi les chances de succès d'éventuelles attaques. D'autres avantages de ce bouton d'alerte ont également été prouvés :

IMPACT DU BOUTON D'ALERTE PHISHING

Taux d'adhésion à la formation en ligne

Pourcentage de personnes ayant terminé le module

Les entreprises peuvent donc aider leurs collaborateurs à acquérir et à perfectionner les compétences et les connaissances dont ils ont besoin pour prendre des décisions éclairées. Il suffit, pour cela, qu'elles leur proposent une formation personnalisée et pertinente, mais aussi leur fournissent les bons outils contextuels. Chaque employé pourra alors constater qu'il joue un véritable rôle dans la défense de la société et poursuivra sa formation en étant mieux conscient de l'importance de son engagement.

Exemples de mesures comportementales relatives au contexte :

- → Taux d'engagement avec/sans personnalisation de la formation
- → Taux d'alerte phishing avec l'outil de signalement intégré
- → Impact de l'utilisation de l'outil de signalement sur le nombre de personnes qui achèvent la formation en ligne

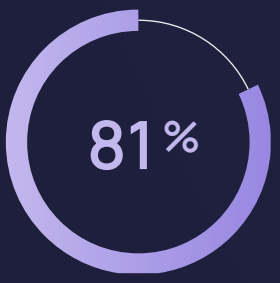
3.3 Motivation : mobiliser les collaborateurs pour de meilleurs résultats

Une entreprise avec une solide culture de la sécurité, c'est une entreprise dont les employés sont mobilisés, impliqués et bien formés. S'il est essentiel d'avoir accès aux outils et aux technologies de formation, il est tout aussi important d'entretenir un environnement réceptif qui implique toute l'entreprise, quelles que soient les fonctions et les responsabilités de chacun. La motivation doit venir de la tête, et se propager à toutes les équipes. C'est pourquoi il est indispensable que les cadres supérieurs se donnent pour mission d'insuffler une culture holistique plutôt que d'établir une sécurité compartimentée. Parmi tous les facteurs internes et externes qui contribuent à la maturité d'une culture de la sécurité, la motivation sort véritablement du lot.

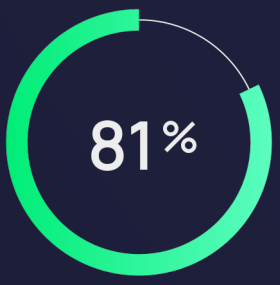
Elle est souvent considérée comme un élément purement qualitatif, non quantifiable. Pourtant, si sa nature multidimensionnelle ne permet pas de la mesurer en tant que telle, il est possible de l'évaluer au moyen de facteurs corrélés tels que les progrès, l'effort et la réussite. Le recours à la gamification, par exemple, stimule fortement l'engagement direct. Il a en effet été prouvé que les formations en ligne gamifiées, qui incluent des modules incitatifs, suscitent davantage d'intérêt, d'intégration et de participation que les sessions traditionnelles de style scolaire. Ce faisant, elles alimentent, sur le long terme, la motivation des collaborateurs. Selon une enquête réalisée par TalentLMS, plus de 80 % des personnes interrogées trouvent que la gamification nourrit la créativité, favorise l'apprentissage et la concentration, et fournit un objectif global.

Au fur et à mesure des progrès et de l'acquisition de connaissances, la motivation est à la fois un élément moteur de la formation et l'un de ses produits. Motivation et apprentissage vont donc de pair et poussent les utilisateurs à l'action.

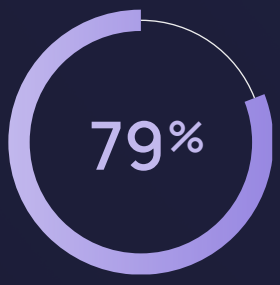
La gamification véhicule une idée **de créativité, de choix, de liberté** et/ou **le sens des responsabilités**



La gamification me donne un **sentiment d'appartenance** avec l'impression d'être mieux **connecté sur le plan social**



La gamification m'aide à apprendre et à me **développer sur le plan personnel et professionnel**



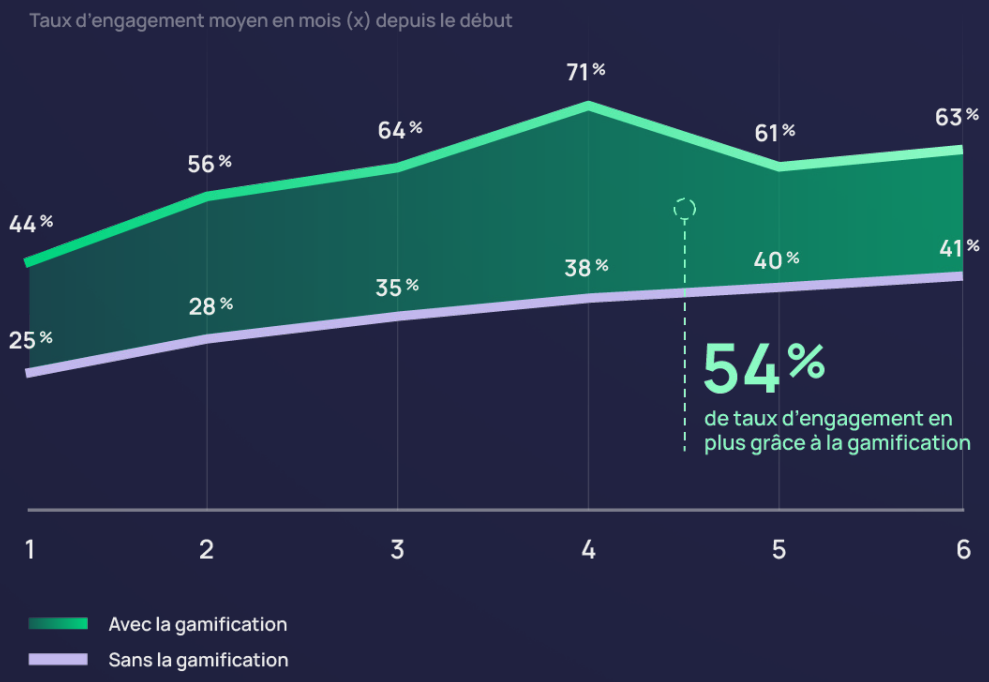
La gamification donne du **sens à la formation** et définit un objectif global au sein de mon environnement de travail

Source :
TalentLMS (2018). The 2018 Gamification At Work Survey.

Il a été prouvé que des plateformes, comme celles de SoSafe, conçues d'après les données et les principes fondateurs des sciences comportementales, stimulent la motivation de manière durable, même sur des sujets aussi complexes que la cybersécurité. En jouant sur une approche narrative passionnante, des défis à relever, des niveaux à gravir et des récompenses bien méritées, la gamification augmente le taux d'engagement des utilisateurs de plus de 50 %. Si les sujets relatifs à la sécurité sont présentés aux collaborateurs sous un jour ennuyeux et complexe, la motivation intrinsèque leur fera défaut. Dans le rythme trépidant de leur quotidien professionnel, ils auront probablement l'impression de ne pas avoir suffisamment de temps pour ces choses. L'intégration d'éléments issus de l'univers des jeux vidéo dans le processus de formation a fait ses preuves : elle augmente le plaisir et favorise l'apprentissage dans la durée.

UTILISATION DU PRODUIT

La gamification stimule l'engagement de l'utilisateur et sensibilise davantage à la sécurité dans une dynamique ludique



Grâce à cette expérience immersive, les apprenants bénéficient d'un retour immédiat, peuvent ainsi se corriger et inscrire les bons gestes dans leurs habitudes. Au fur et à mesure de leur progression, des récompenses stimulent leur motivation.

Exemples de mesures pour évaluer la motivation :

- → Taux d'engagement dans la formation en ligne
- → Impact de la gamification sur le nombre de personnes qui achèvent la formation en ligne

3.4 Comportement : pour que la sécurité devienne une seconde nature

Le pivot de toute culture solide de la sécurité est le comportement. C'est d'ailleurs ce qui ressort de toutes les mesures évoquées précédemment. Prendre le temps de verrouiller son écran lorsqu'on s'éloigne de son ordinateur, procéder à une analyse de ses e-mails pour repérer d'éventuelles activités suspectes et informer le service informatique des risques et des incidents rencontrés de manière proactive : toute la protection de votre entreprise passe par l'instauration de bonnes habitudes dans la routine de vos collaborateurs. Mesurer l'évolution des comportements au fil de la formation permet d'adapter le programme en conséquence tout en réduisant efficacement les risques cyber.

Comme vous l'avez probablement déjà compris, l'adoption de telles habitudes numériques dans le contexte (professionnel) quotidien dépend fortement des trois autres variables : ces réflexes de sécurité ne s'installeront sur le long terme que si vos collaborateurs ont des connaissances en sécurité de l'information, si ces connaissances sont correctement adaptées au contexte et si la motivation intrinsèque est stimulée. Que ce soit l'impact de la répétition espacée sur la rétention des informations, celui de la motivation pour stimuler les taux d'engagement ou celui de la contextualisation de la formation sur l'augmentation du taux d'alerte phishing… toutes ces mesures montrent bien que la culture de la sécurité mérite une approche plus holistique. Se contenter de cibler l'un de ces aspects ou de cocher les cases des exigences réglementaires en organisant une présentation ponctuelle sur site autour de la cybersécurité ne permet plus de relever efficacement les défis que pose l'évolution constante des menaces, aujourd'hui.

Il faut, au contraire, que les décisionnaires jouent sur tous les tableaux de ce modèle de sécurité comportementale afin de mettre en place un programme de sensibilisation adapté qui fera de la cybersécurité, une seconde nature chez leurs employés.

Exemples de mesures pour évaluer le comportement :

- → Taux d'alerte phishing via l'outil de signalement
- → Taux d'interaction avec les e-mails et les pages de simulation de phishing
- → Taux d'utilisation quotidienne ou hebdomadaire d'un gestionnaire de mots de passe
- → Taux de clics différenciés en fonction des tactiques psychologiques utilisées
- → Délai de signalement

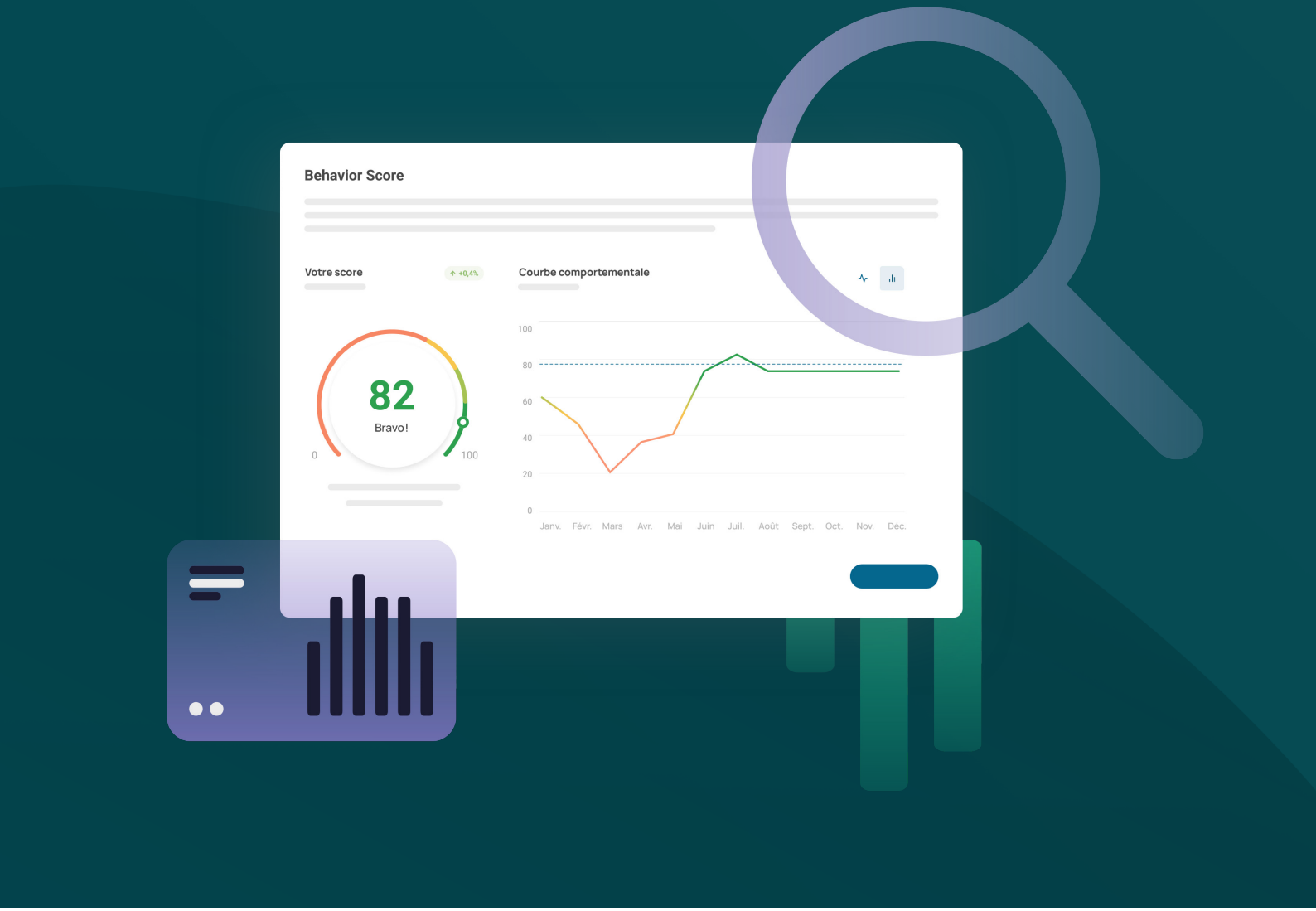
04 Pourquoi la mesure des comportements est une pratique qui porte ses fruits en cybersécurité

Ce qui fait la force d'une culture de la sécurité, c'est la convergence de tous les facteurs qui favorisent l'adoption de comportements vigilants. Pour renforcer ses défenses, l'entreprise doit adopter une stratégie en adéquation avec le niveau d'expertise de ses employés et avec les risques auxquels ils sont exposés. Notre modèle de sécurité comportementale montre bien que chacun des facteurs - la connaissance, le contexte, la motivation et le comportement - interagit constamment avec les trois autres pour former la base de toute stratégie moderne de cybersécurité, au-delà de toutes les listes de « cases à cocher ».

Loin des méthodes de formation traditionnelles, il propose une expérience immersive, incitative et surtout efficace, donnant toutes les clés nécessaires aux collaborateurs. L'évolution des comportements est mesurable, et donc prouvée. Identifiez les forces et les faiblesses en matière de cybersécurité grâce à un programme de formation en adéquation avec vos objectifs d'entreprise. Il vous permettra de mesurer les paramètres les plus pertinents pour vous. Au lieu d'avancer à l'aveugle dans ce domaine, les décisionnaires devraient eux-mêmes adopter une approche proactive de la sécurité, montrant ainsi l'exemple à leurs équipes.

Ne laissez plus les différents paramètres au hasard, en supposant que tant d'employés savent et qu'ils réagiront de telle ou telle manière en cas d'attaque. Établissez plutôt un programme de sensibilisation à la cybersécurité qui forme, enseigne et remédie à toute forme de négligence pour instaurer de bonnes habitudes. Mesurez ces évolutions pour connaître les points précis sur lesquels votre entreprise doit s'améliorer. Tout au long de ce processus, les collaborateurs gagnent en savoir-faire et voient leur participation récompensée alors qu'ils contribuent à garantir bien plus que des données : des connaissances.

Dans les solutions de sensibilisation de nouvelle génération, comme celle de SoSafe, le recueil des mesures comportementales permet de se faire une idée des fruits que porte la formation, mais aussi des vulnérabilités qu'elle a mises en évidence et auxquelles il faut remédier au plus vite. Elles vont plus loin encore : elles vous accompagnent, à l'aide de conseils sur les risques cyber, pour vous aider à identifier, comprendre et endiguer les menaces auxquelles vous êtes exposés.



Quel est votre Behavior Score[BETA] ?

Le Behavior Score est un indicateur de performance en matière de phishing. Il est conçu pour répondre à trois des questions qui reviennent les plus souvent chez les responsables de la sécurité informatique :

1. Quelle est la probabilité que mon entreprise soit victime de phishing ou d'ingénierie sociale ?
2. Comment dresser facilement, pour les cadres supérieurs, un bilan rapide des performances de nos collaborateurs sans trop entrer dans les détails ?
3. Que puis-je faire pour améliorer notre score et aller au-delà des standards du secteur ?

Mode de fonctionnement

Actuellement disponible en version Beta, le Behavior Score évalue les entreprises sur la base de trois mesures différentes, recueillies dans le cadre des simulations de phishing : le taux de clics, le taux d'interaction et le taux de signalement (pour les utilisateurs de notre bouton d'alerte phishing). Ce score s'affiche sous la forme d'un nombre compris entre 0 et 100. Si nous disposons d'informations suffisantes, vous verrez également apparaître le score moyen des 20 entreprises les plus performantes de votre secteur d'activité.

TAUX D'INTERACTION

Interactions avec des simulations de sites Internet frauduleux, par exemple saisie d'identifiants de connexion

TAUX DE CLICS

Clics sur le lien contenu dans un faux e-mail de phishing

TAUX DE SIGNALEMENT

Simulations de phishing signalées par le bouton d'alerte phishing

Votre score et ce qu'il dit de votre situation actuelle

En construction
<58

Vos employés interagissent plus que la moyenne (dans votre secteur) avec les simulations de phishing. Ce comportement fragilise votre entreprise face aux menaces. Redoublez d'efforts en matière de sensibilisation à la sécurité des e-mails pour combler efficacement ces lacunes, sans tarder.

Solide
58-68

Vos résultats sont dans la moyenne de votre secteur d'activité. Vous avez su établir des bases solides. Familiarisez vos collaborateurs à des formes d'attaque plus sophistiquées (le spearphishing personnalisé, par exemple) pour renforcer encore votre pare-feu humain.

Forte
69-77

La capacité de votre entreprise à identifier et prévenir les attaques de phishing est au-dessus de la moyenne. Il est temps, si ce n'est déjà fait, de compléter votre solide culture de la sécurité par des habitudes de signalement bien établies.

Experte
77+

Félicitations ! Peu d'entreprises parviennent à ce niveau. Votre score prouve que votre société possède une solide culture de la sécurité. Votre nouvelle mission est tout aussi ambitieuse que passionnante : maintenir l'engagement et les habitudes de sécurité au plus haut niveau.

Développez une culture de la cybersécurité, au sein de votre entreprise, en toute simplicité !

La plateforme de sensibilisation SoSafe permet aux entreprises de consolider leur culture de la sécurité en limitant les risques humains. Elle propose une expérience d'apprentissage stimulante ainsi que des simulations d'attaques personnalisées qui enseignent aux employés comment protéger activement la société des menaces en ligne. Chaque outil est développé selon les principes des sciences comportementales pour assurer une formation à la fois ludique et efficace. Des analyses détaillées mesurent les fruits de ce programme en matière d'évolution des comportements et révèlent précisément aux sociétés les lacunes à combler pour assurer une réponse proactive face à d'éventuelles menaces. Facile à déployer et évolutive, la plateforme de SoSafe inscrit en chaque employé des réflexes de sécurité, sans lui demander d'efforts démesurés.

Micro-apprentissage stimulant

Une plateforme de formation inspirée des sciences comportementales qui enthousiasme les collaborateurs :

Améliorez votre résilience face aux menaces cyber et assurez votre conformité aux obligations légales grâce à une formation dynamique et percutante qui joue sur différents canaux pour développer, sans efforts, des réflexes de sécurité qui durent.

- → Une pédagogie narrative et gamifiée conçue pour favoriser l'engagement et la mémorisation
- → Une bibliothèque de contenus présélectionnés prêts à être implémentés pour faire évoluer votre formation
- → Des options de personnalisation et de gestion de contenu qui ne demandent que peu d'efforts et s'adaptent à chaque entreprise

Simulations de spearphishing

Simulations de phishing axées sur l'utilisateur pour développer des réflexes de sécurité :

Apprenez à vos employés à traquer les cyberattaques à l'aide de simulations de spearphishing automatisées qui renforcent durablement leur vigilance au quotidien : un moyen efficace pour réduire les risques et le temps de signalement des menaces dans une situation où chaque minute peut compter.

- Des simulations de cyberattaques personnalisées et réalistes
- Des explications pédagogiques contextualisées qui consolident les habitudes de sécurité des employés
- Un bouton d'alerte phishing intégré pour signaler les menaces en un seul clic

Suivi stratégique des risques

Le tableau de bord offre une vue d'ensemble des risques humains et permet de réagir de manière proactive aux éventuelles vulnérabilités :

Appuyez-vous sur des analyses détaillées qui vous donnent une vue d'ensemble des risques auxquelles votre entreprise est exposée. Suivez et orientez l'impact de votre programme de sensibilisation sur l'évolution des comportements, puis prenez des décisions éclairées, sur la base des données dont vous disposez.

- Un suivi des données contextuelles avec ICP techniques et psychologiques
- Des références propres au secteur de l'entreprise et des informations pratiques sur les principaux axes d'amélioration
- Une solution développée pour répondre aux exigences de la norme ISO/CEI 27001 et conçue selon une approche de « privacy by design »

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Allemagne

info@sosafe.de
www.sosafe-awareness.com/fr
+49 221 65083800