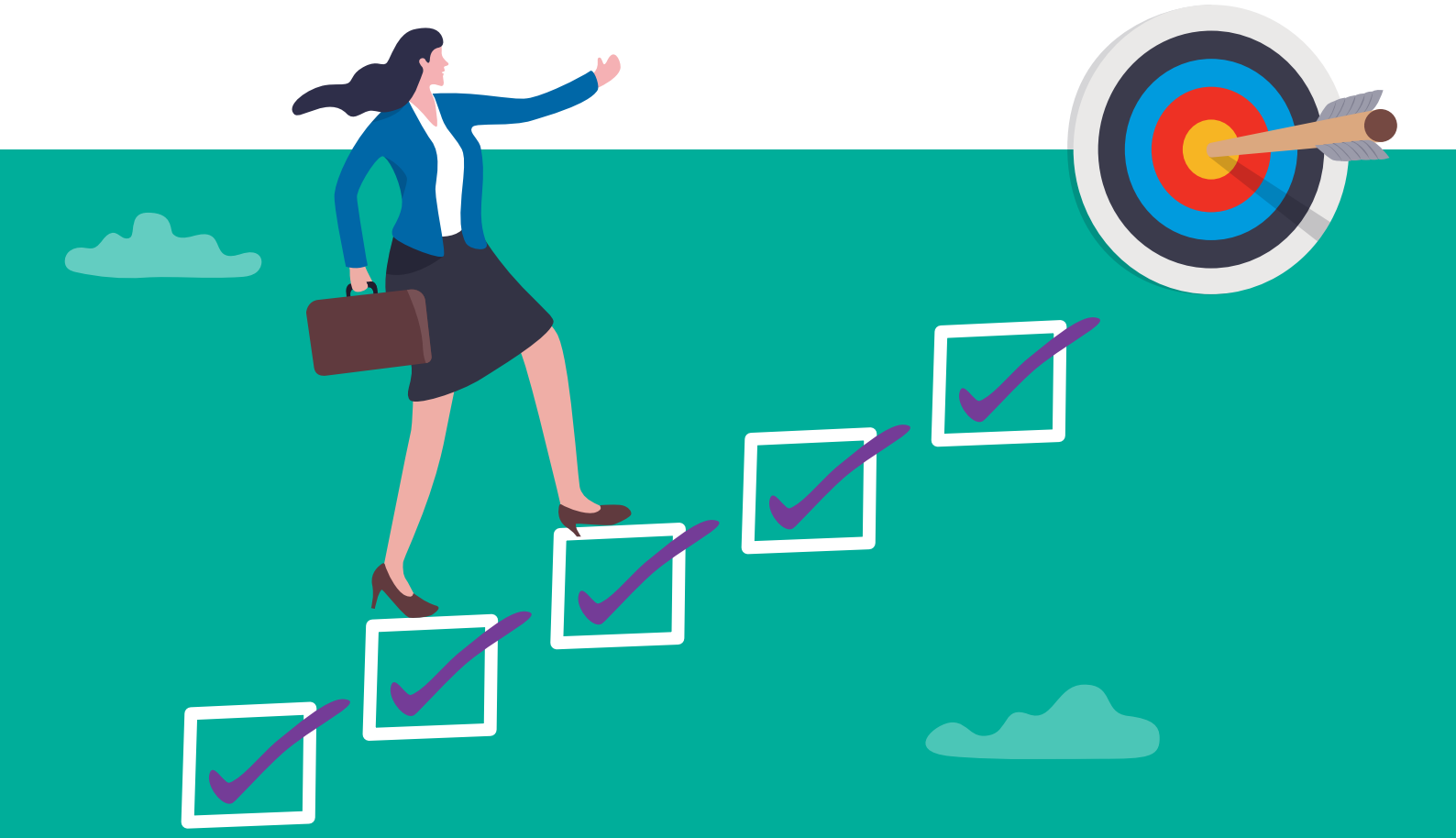
proofpoint.

EBOOK

ÉDITION 2023

Mise en œuvre d'un véritable changement des comportements

Guide de conception d'un programme de sensibilisation à la sécurité informatique qui fonctionne réellement



proofpoint.com/fr

Les personnes au cœur de vos projets de cybersécurité

Aujourd'hui, la cybermenace la plus dangereuse n'est pas une vulnérabilité Zero-Day, un nouveau malware ou encore le dernier kit d'exploitation. Ce sont vos propres utilisateurs.

En effet, les attaques d'aujourd'hui ciblent les personnes, et non l'infrastructure informatique. Quelle que soit leur forme, la plupart des cyberattaques ont besoin de l'intervention d'une victime pour être activées. Leur but est d'inciter des personnes à ouvrir des pièces jointes malveillantes, à cliquer sur des URL dangereuses, à communiquer des identifiants de comptes, voire à agir directement, par exemple en effectuant un virement ou en envoyant des données sensibles.

Importance de la formation des utilisateurs

Selon le rapport d'enquête 2022 sur les compromissions de données, 82 % des compromissions impliquent une intervention humaine. Comme le précise le rapport, les malwares et les identifiants de connexion dérobés entrent en jeu dans un second temps, une fois qu'une attaque d'ingénierie sociale a ouvert la porte aux cybercriminels, ce qui souligne l'importance d'un programme robuste de sensibilisation à la sécurité informatique[1].

Les formations de sensibilisation des utilisateurs constituent l'une des principales mesures à prendre pour sécuriser votre entreprise. En apprenant à vos utilisateurs à identifier, rejeter et signaler les tentatives de phishing, vous pouvez ériger une dernière ligne de défense robuste contre les cybermenaces les plus dangereuses d'aujourd'hui.

Objectif de ce guide

La mise en place d'un nouveau programme de formation peut être difficile. Faire en sorte qu'il intéresse vos utilisateurs, change véritablement leur comportement et limite l'exposition de l'entreprise aux menaces dans le temps peut constituer un défi encore plus grand.

Nous sommes là pour vous aider.

Ce guide vous explique comment créer et conserver un programme de formation à la cybersécurité efficace, indépendamment de sa maturité, du fournisseur ou des obstacles que vous pourriez rencontrer. Il propose des faits essentiels, des stratégies efficaces, des ressources utiles et des conseils pratiques pour les responsables de la sécurité, à chaque étape du parcours de sensibilisation à la sécurité informatique.

Voici quelques exemples de questions auxquelles nous vous aiderons à répondre :

- Comment obtenir l'adhésion des personnes concernées ? Avec qui dois-je travailler en interne ?
- Que dois-je faire ? À quelle fréquence ?
- Comment m'assurer de la participation de mon personnel ?
- Comment puis-je mesurer et partager le succès du programme ?

82 %

des compromissions impliquent une intervention humaine[1].

1 Verizon, « 2022 Data Breach Investigations Report » (Rapport d'enquête 2022 sur les compromissions de données), juin 2022.

Modèle de mesure et de limitation du risque utilisateur centré sur les personnes

Si chaque personne est unique, sa valeur aux yeux des cybercriminels et les risques qu'elle représente pour l'entreprise le sont également. Proofpoint a élaboré un modèle VAP™ (Very Attacked People, ou personnes très attaquées) pour mesurer et limiter trois aspects distincts du risque utilisateur.

Les formations de sensibilisation à la sécurité informatique sont directement liées à la vulnérabilité de l'utilisateur. Mais votre programme doit également prendre en compte le profil d'attaque des utilisateurs et leurs privilèges. Ces informations vous aideront à adopter une approche de sensibilisation à la sécurité informatique centrée sur les personnes qui inclut des formations de suivi adaptées, proactives et ciblées.

V

Vulnérabilité

Ce critère évalue la probabilité que l'utilisateur se laisse abuser en cas d'attaque, en raison de sa susceptibilité aux tactiques des cybercriminels ou d'habitudes en ligne dangereuses. Cette vulnérabilité peut être mesurée par des évaluations des connaissances, des tests réalisés dans le cadre des formations de sensibilisation à la sécurité informatique et des simulations d'attaques de phishing.

A

Profil d'attaque

Ce critère quantifie le volume et la sophistication des attaques et des cybercriminels ciblant l'utilisateur. Il peut également prendre en compte des utilisateurs associés ou similaires au sein de l'entreprise ou en dehors.

P

Privilèges

Ce critère permet de déterminer la valeur et la sensibilité des données, systèmes et ressources auxquels l'utilisateur a accès. Il peut également être considéré comme une méthode de mesure des dégâts potentiels en cas de réussite d'une attaque contre cet utilisateur.

Sommaire

SECTION 1

Ce qu'il faut savoir avant de commencer

C'est fait. Vous avez enfin trouvé un fournisseur pour vos formations de sensibilisation à la sécurité informatique. Ce dernier vous envoie un lien vers la solution logicielle choisie et le monde est à vous. Vous voici prêt à lancer des simulations d'attaques de phishing, à collecter des données, à attribuer des formations et à utiliser tous les contenus et fonctionnalités incroyables découverts lors des démonstrations du produit.

Vous envoyez un message concernant le lancement de votre programme de sensibilisation à la sécurité. Subitement, votre boîte de réception se retrouve submergée de réponses de ce type :

- Qui a approuvé ce projet ?
- Je vais en parler à mon supérieur.
- Ai-je vraiment besoin d'un tel programme ?

Il s'agit là des premiers obstacles généralement rencontrés par nos clients. Mais ils montrent aussi la voie à suivre pour garantir le succès d'un programme de sensibilisation à la sécurité : obtenir l'adhésion des utilisateurs.

Une remarque récurrente des clients est le refus de certains utilisateurs de participer à des formations de sensibilisation à la sécurité informatique.

Obtenir l'adhésion des utilisateurs

Une remarque récurrente des clients est le refus de certains utilisateurs de participer à des formations de sensibilisation à la sécurité informatique. Peut-être les simulations d'attaques donnent-elles aux utilisateurs un sentiment de vulnérabilité. Ou peut-être considèrent-ils les formations comme un autre exercice d'entreprise et une distraction qui les détourne de leur « véritable » travail.

Voici quelques solutions pour surmonter ce type d'obstacles :

Communiquez en gardant à l'esprit les avantages pour l'utilisateur. Lorsque vous rédigez des communications à l'intention des utilisateurs, pensez à la question qu'ils vont se poser : « Qu'est-ce que cela m'apporte ? ». Donnez-leur des exemples concrets, tels que l'usurpation d'identité, le vol de cartes de crédit, les compromissions de comptes et d'autres exemples de ce type. Montrez-leur ce que les formations peuvent leur apporter dans leur vie personnelle. Le programme en deviendra plus intéressant à leurs yeux et ils participeront davantage.

Trouvez le juste équilibre entre évaluations et formations. Les évaluations de simulations d'attaques de phishing sont des composants appréciés des programmes. Mais elles sont parfois trop utilisées. De nombreux clients nous ont fait part du besoin de trouver un juste équilibre entre les évaluations et les activités de formation et de sensibilisation. Comme nous l'a fait remarquer un client : « Si nous envoyons uniquement des simulations d'attaques de phishing, les utilisateurs pensent que nous cherchons à les piéger. » Il convient de trouver un compromis entre simulations et évaluations dans un programme, de même qu'y intégrer des activités de sensibilisation et autres (par exemple, des concours).

Arborez un visage avenant et souriant lors des événements d'entreprise. Les formations et les évaluations assistées par ordinateur peuvent avoir un côté impersonnel. Pensez à avoir un stand lors des grands événements de l'entreprise ou à organiser des sessions virtuelles, telles que des webinaires, qui apportent une touche plus personnelle. Commencez par une réunion de lancement avec les collaborateurs, organisez des événements de formation et proposez des ressources utiles.
Vous pouvez aussi envisager de distribuer des cadeaux ou simplement d'offrir un café. Cette approche permet d'humaniser le programme, de le rendre plus convivial.

Surmonter la résistance

Il ressort des conversations avec les clients que les utilisateurs non impliqués relèvent généralement de deux catégories :

- **Récidivistes :** utilisateurs qui échouent systématiquement aux simulations d'attaques de phishing et autres évaluations
- **Non-participants :** utilisateurs qui refusent de prendre part aux formations

Vous pensez avoir tout tenté pour convaincre ces utilisateurs — emails, discussions en personne, entretiens avec les responsables, voire suppression de leur accès réseau. Même si vous ne pouvez toujours pas changer leur comportement, il vous reste d'autres solutions.

La stratégie d'un de nos clients consistait à demander au RSSI ou à un autre cadre supérieur de prévoir 15 minutes dans l'agenda de ces utilisateurs pour discuter des thèmes suivants :

- L'importance du comportement de l'utilisateur et de la sensibilisation à la sécurité informatique
- Les moyens mis en œuvre par le département pour tenter de protéger l'entreprise et les utilisateurs dans des situations personnelles
- Les raisons pour lesquelles le collaborateur doit s'engager à faire preuve de plus de vigilance ou à participer à des formations

Ce type d'interaction laisse une forte impression. Il communique l'importance d'adopter les bons comportements et de participer plus activement, de façon plus personnelle et concrète.

Le signalement du phishing par les utilisateurs : une arme à double tranchant

Lors de l'une de nos conférences annuelles, un client a émis le commentaire suivant après une présentation.

« Mes utilisateurs ne signalent pas les emails de phishing à notre boîte email de signalement d'abus ». Ils n'envoient que des messages légitimes ou du spam. Notre équipe ne parvient plus à suivre. Comment pouvons-nous résoudre ce problème ? »

Les boîtes email de signalement d'abus offrent un moyen efficace de limiter le risque. Leur gestion demande toutefois un temps considérable. Nous avons trouvé deux solutions à cet obstacle courant :

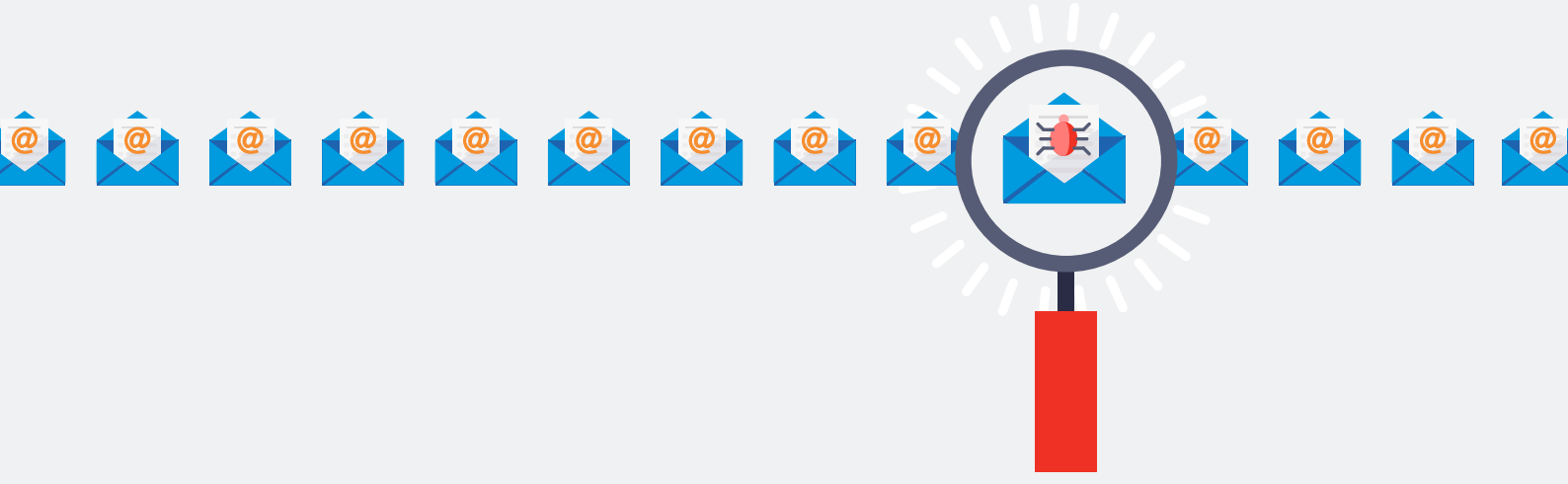
- Aider les utilisateurs à mieux détecter les véritables emails de phishing
- Automatiser le processus d'analyse et de réponse aux emails de phishing signalés

Un programme efficace de sensibilisation à la sécurité informatique conduira naturellement à un meilleur signalement des menaces. De nombreux clients constatent une amélioration du signalement (davantage de messages réellement malveillants et moins de faux positifs) entre 6 à 12 mois après le déploiement d'un programme cohérent qui forme les utilisateurs à identifier les emails de phishing.

L'automatisation de l'analyse et de la réponse aux emails peut alléger la charge de travail par l'analyse et l'enrichissement automatiques via le sandboxing et la threat intelligence. L'équipe informatique est moins sollicitée grâce à la suppression automatique du contenu malveillant des boîtes de réception des utilisateurs et à l'exclusion des faux positifs.

Autre avantage d'une réponse automatisée : les utilisateurs peuvent recevoir un feedback automatique leur indiquant si le message signalé était réellement malveillant. Cette mesure permet aux utilisateurs d'apprendre et améliore la sécurité en renforçant les comportements positifs par un simple merci lors du signalement d'emails malveillants.

Un programme efficace de sensibilisation à la sécurité informatique conduira naturellement à un meilleur signalement des menaces.



SECTION 2

Timing du programme

Le timing n'est pas un détail anodin de votre programme de formation et de sensibilisation à la sécurité informatique : il représente la somme de tous vos efforts. Un programme ne sera déployé « au bon moment » que s'il combine les bonnes formations et les bonnes personnes, ainsi que de nombreux autres éléments tactiques, organisationnels et stratégiques.

Chaque entreprise est unique et chaque programme sera donc différent. Mais tous doivent inclure les éléments suivants :

- Définition des besoins de formation
- Identification des utilisateurs présentant des besoins de formation spécifiques
- Définition des activités
- Élaboration et gestion des calendriers
- Communication et test des premières étapes
- Définition de la fréquence et du timing des activités du programme

Ordre recommandé des activités : liste de contrôle

Le succès de votre programme va dépendre du soin que vous mettez à le concevoir et d'une bonne planification. Les étapes clés suivantes se sont avérées très utiles pour nos clients.

Un principe clé de la cybersécurité centrée sur les personnes est que chaque utilisateur est unique.

1. **Définition des besoins de formation.**

   Une stratégie de cybersécurité centrée sur les personnes commence par la mesure du risque utilisateur. Les évaluations des utilisateurs fournissent de précieux renseignements sur les principales vulnérabilités des utilisateurs et sur les formations qu'ils doivent suivre pour améliorer leur connaissance de thèmes essentiels tels que le phishing, la protection des données, la sécurité des terminaux mobiles et bien plus encore.

   En vase clos, le risque n'existe pas. Pour identifier les besoins de formation, il faut avant tout comprendre le paysage des menaces actuel. C'est là que la threat intelligence joue un rôle essentiel. Une threat intelligence réelle et récente aide à comprendre les menaces actuelles et émergentes que les utilisateurs sont susceptibles de rencontrer.

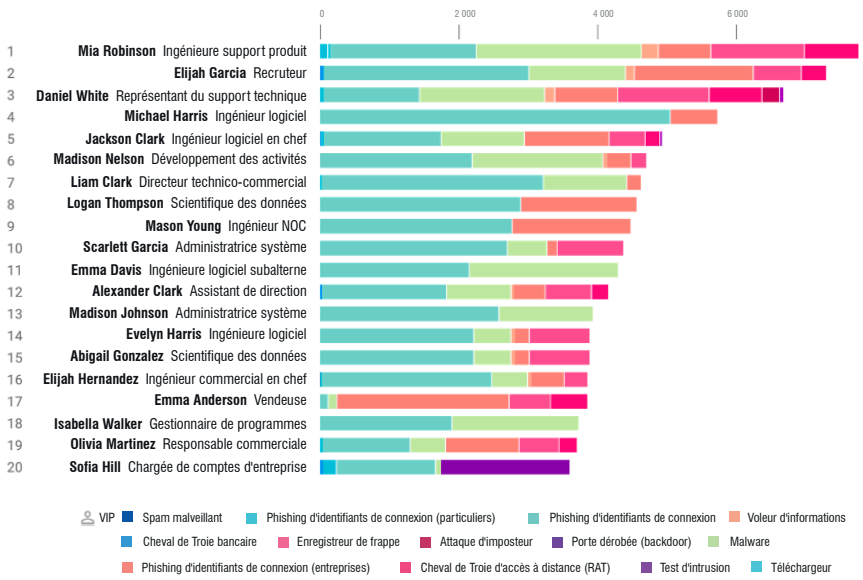
2. **Identification des utilisateurs et des groupes nécessitant une formation ou un programme de formation adapté à leurs besoins.**

   Un principe clé de la cybersécurité centrée sur les personnes est que chaque utilisateur est unique. Une approche de protection universelle ne fonctionne pas dans l'environnement actuel, en ce compris pour les programmes de sensibilisation à la sécurité informatique.

   Les groupes suivants peuvent nécessiter des formations adaptées ou spécialisées :

   - VAP **:** les utilisateurs posant un risque élevé car particulièrement vulnérables aux tactiques des cybercriminels sont plus fréquemment pris pour cible lors d'attaques, ou ont accès à des données, systèmes ou ressources de valeur.

Rapport sur les VAP généré par Proofpoint Targeted Attack Protection



- VIP : les membres de l'équipe de direction ou du conseil ainsi que les personnes occupant d'autres postes à responsabilité peuvent avoir besoin d'une formation et de conseils spécifiques en raison de leur importance pour l'entreprise. De nombreux VIP peuvent également être des VAP.
- Rôles et départements internes précis : les collaborateurs des services RH, financier, juridique, de conformité, de développement ou d'autres rôles peuvent être tenus de suivre des formations spécifiques ou obligatoires d'un point de vue légal. Envisagez des évaluations des connaissances et des simulations différentes pour ces groupes à mesure que votre programme de formation gagne en maturité.

3. **Détermination des activités clés à inclure dans votre programme.**

   Pour être efficace, un programme de formation doit trouver le juste équilibre entre évaluations, formations, ressources de formation, communications et activités virtuelles ou en personne. Voici quelques éléments qu'il serait utile d'inclure au vôtre :

   - Évaluations des utilisateurs pour déterminer leurs connaissances et vulnérabilités. Ces évaluations peuvent inclure des simulations d'attaques de phishing, de SMiShing (phishing par SMS/texte) et par clés USB.
   - Formations assistées par ordinateur basées sur les besoins des utilisateurs et le paysage actuel des menaces
   - Activités de sensibilisation (posters, webinaires, newsletters, vidéos) pour présenter différents concepts et renforcer les messages clés
   - Activités virtuelles et en personne, par exemple des déjeuners de présentation ou des webinaires. Faites preuve de créativité. Par exemple, certains de nos clients ont créé des « escape games » de cybersécurité qui ont très bien marché.

4. **Test et communication des premières étapes.**

   Pour de nombreuses entreprises, un programme complet de formation des utilisateurs peut représenter un changement majeur. Commencez par un petit groupe d'utilisateurs afin de régler les problèmes éventuels. Annoncez les premières étapes à l'ensemble des personnes concernées à un stade précoce et à intervalles fréquents. Limitez les surprises.

   Deux mois avant le lancement

   Envoyez une simulation d'attaque de phishing test à un petit groupe de personnes « informées » pour mettre au jour d'éventuels problèmes techniques cachés. Ensuite, envoyez un test de phishing de référence moyennement difficile à tous les collaborateurs.

   À ce stade, redirigez les utilisateurs qui se font piéger par votre leurre de phishing vers un site « 404 - page introuvable ». (Par la suite, redirigez ceux qui cliquent sur l'email de phishing vers une page de renvoi « didactique ».)

   Un mois avant le lancement

   Annoncez le programme aux utilisateurs. Si vous déployez un module d'extension de signalement d'emails, expliquez à quoi il va servir et comment l'utiliser.
   Et si vous avez accès à du contenu comme des posters, des images ou d'autres supports de sensibilisation à la sécurité informatique, placez-les un peu partout dans l'entreprise ou publiez-les sur un wiki consacré à votre programme.

5. **Définition de la fréquence et du timing des activités du programme.**

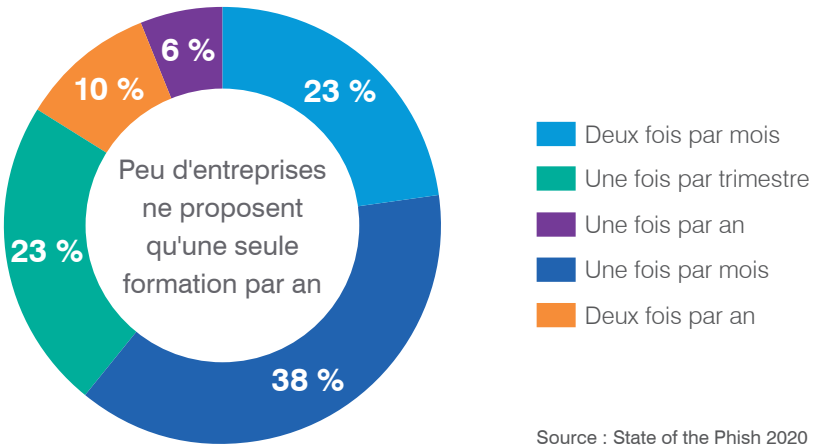
   Une fois encore, tout est question de timing. Nous recommandons d'organiser les activités de sensibilisation à la sécurité informatique aux intervalles suivants :

   - Envoyez un test de phishing toutes les quatre à six semaines. Pensez à varier les types de thèmes et de leurres utilisés.
   - Utilisez l'inscription automatique aux tests de phishing au moins une fois par trimestre. Utilisez un module de formation de suivi ciblé, selon le type d'attaque envoyé.
   - Examinez les rapports sur les VAP une ou deux fois par mois. Selon les résultats des rapports, déterminez qui doit recevoir une formation ciblée et le contenu de formation à utiliser.
   - Attribuez des formations à l'ensemble du personnel de l'entreprise au moins une fois par trimestre.
   - Répétez les évaluations globales des connaissances et les tests de phishing au moins une fois par an pour les comparer aux évaluations de référence.
   - Pour renforcer la rétention des connaissances, planifiez des activités de sensibilisation à la sécurité informatique au moins deux fois par an, notamment des webinaires, des concours ou (si possible) des activités en personne.

Créez un cadre annuel pour organiser les composants et le calendrier des activités de formation. Faites preuve de souplesse et adaptez le calendrier en fonction de l'évolution du paysage global des menaces.

Notre rapport State of the Phish 2020 révèle que la formation de sensibilisation à la sécurité informatique a progressé : d'une activité annuelle et trimestrielle, elle est devenue un événement mensuel, voire bimensuel. Nous recommandons des formations mensuelles ou plus fréquentes, y compris des formations ciblées, des campagnes de sensibilisation et des évaluations des connaissances.

Fréquence des formations de sensibilisation à la sécurité informatique



Source : State of the Phish 2020

Le paysage des menaces ne cesse d'évoluer. C'est la raison pour laquelle votre programme de sensibilisation à la sécurité informatique doit être continu, et non ponctuel.

Quand le modifier

Le paysage des menaces ne cesse d'évoluer. C'est la raison pour laquelle votre programme de sensibilisation à la sécurité informatique doit être continu, et non ponctuel. En comparant l'évaluation de référence initiale aux suivantes, vous pouvez suivre l'amélioration des connaissances des utilisateurs et ainsi prévoir des solutions pour réduire les risques.

Voici quelques situations nécessitant de revoir la fréquence ou l'ordre de vos activités de formation :

- **Lorsque la prévalence de certaines menaces spécifiques augmente ou que les cybercriminels utilisent une marque ou un leurre précis.** Modifiez le contenu des évaluations, par exemple les modèles de simulation d'attaque de phishing, ou utilisez un contenu didactique basé sur les menaces en circulation pour mieux gérer le risque.
- **Si votre entreprise est confrontée à un incident, tel qu'une compromission de données.** Envisagez d'actualiser les activités planifiées et la fréquence des communications, évaluations et formations en rapport avec cet incident.
- **Si de nouvelles législations ou réglementations exigent des formations supplémentaires.** Faites en sorte que ces formations soient suivies d'une évaluation des connaissances pour savoir dans quelle mesure les utilisateurs ont assimilé le contenu de ces formations.
- **Lorsque votre entreprise publie ou met à jour des règles ou n'est pas sûre que ses collaborateurs en aient pris connaissance.** Une évaluation personnalisée des connaissances peut vous aider à identifier les lacunes des utilisateurs et à orienter les initiatives de formation.
- **Si un programme de sensibilisation à la sécurité informatique a été interrompu pendant plus de six mois.** Dans ce cas, il peut être judicieux de relancer le programme pour s'assurer que les utilisateurs comprennent son contexte et son importance.

Il est déconseillé de trop augmenter la fréquence des formations, même avec les récidivistes peu intéressés par les évaluations. Des évaluations de phishing mensuelles et l'inscription sélective des utilisateurs qui « échouent » à une formation précise représentent une approche raisonnable et ciblée. Mais attribuer à ces utilisateurs quatre sessions de formation peut s'apparenter à une punition, et ils risquent de s'en agacer.

Surtout, n'essayez pas de tout faire en même temps. Commencez par une analyse appropriée, en vous aidant de la threat intelligence et des évaluations. À partir de là, passez en revue tous les niveaux de l'entreprise pour concevoir un plan réaliste auquel tout le monde peut adhérer.

SECTION 3

L'importance de l'engagement

Les formations de sensibilisation à la sécurité informatique représentent par nature une initiative centrée sur les personnes. Elles visent à donner aux utilisateurs les moyens de reconnaître les attaques dont ils sont les cibles et à changer leur comportement.

C'est pourquoi il est essentiel de préserver l'intérêt des utilisateurs si vous voulez que votre programme soit un succès. Malheureusement, même les programmes les mieux intentionnés peuvent devenir pénibles s'ils n'offrent pas une expérience attrayante et pertinente aux utilisateurs.

Il est essentiel de préserver l'intérêt des utilisateurs si vous voulez que votre programme soit un succès.

Les programmes les plus performants :

- Utilisent un label pour que les utilisateurs se rendent compte de leur pertinence
- S'appuient sur des principes d'apprentissage éprouvés pour changer les comportements
- Renforcent la formation par toute une série de contenus et de supports
- Font appel à des « promoteurs » dans toute l'entreprise dans un but de soutien et d'amélioration
- Guident les utilisateurs grâce à un juste équilibre entre incentives et conséquences

Considérez ces cinq principes comme les piliers d'un programme efficace auquel vos utilisateurs adhéreront. Des clients issus d'un large éventail de secteurs ont utilisé ces concepts pour créer des programmes de formation et de sensibilisation à la sécurité informatique capables de réduire les risques, diminuer les coûts et garantir la conformité aux impératifs de confidentialité des données.

Labellisation du programme

Le choix d'un nom approprié peut aider les utilisateurs à comprendre l'objectif de votre programme de formation et de sensibilisation à la sécurité informatique et les raisons d'y adhérer.

Par exemple, des utilisateurs de l'entreprise peuvent être amenés à traiter des données de clients de l'Union européenne dans le plus strict respect du règlement général sur la protection des données (RGPD). Un titre quelconque et facile à oublier comme « Formation sur le RGPD » risque de susciter peu d'intérêt chez les utilisateurs dont vous aimeriez voir changer le comportement.

Il serait sans doute préférable d'opter pour un titre de type « Devenez un défenseur de la confidentialité des données ». Un tel titre met clairement en avant l'objectif du programme (garantir la confidentialité des données) et le rôle de l'utilisateur (qui participe activement au respect de la confidentialité).

La culture de votre entreprise peut nécessiter une approche plus directe, avec des thèmes plus concrets. Même dans ce cas, attribuer aux programmes des noms en rapport avec le sujet (par exemple, le phishing, l'ingénierie sociale, la messagerie électronique, le télétravail) est un plus.

Utilisation des principes pédagogiques éprouvés

Votre programme doit s'appuyer sur des principes et méthodes pédagogiques reconnus pour obtenir des résultats optimaux en termes d'apprentissage, de rétention et de changement de comportement. Un programme bien conçu propose des connaissances tant conceptuelles que procédurales afin d'offrir aux utilisateurs une vue d'ensemble et des leçons spécifiques. Voici quelques techniques éprouvées :

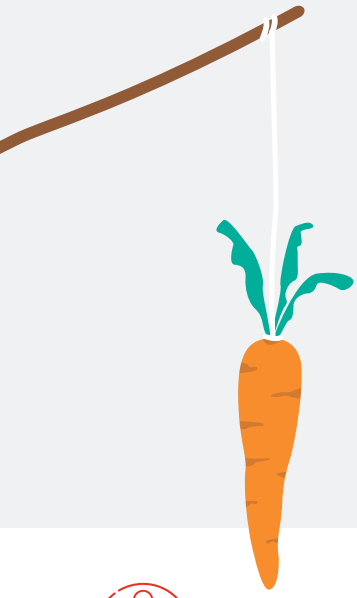
- **Distillez les connaissances à petites doses.** Limitez la durée de la formation à quelques minutes (au lieu de plusieurs heures) et concentrez-vous sur un seul thème dans la mesure du possible.
- **Renforcez les acquis.** Proposez un feedback et organisez régulièrement des activités de formation et de sensibilisation.
- **Formez le personnel en contexte.** Attribuez des formations adaptées aux rôles et aux menaces.
- **Donnez un feedback immédiat.** Communiquez directement les résultats de la formation ou des exercices de phishing.
- **Adaptez-vous au rythme des utilisateurs.** Chaque personne est unique et apprend à un rythme différent.
- **Racontez une histoire.** Proposez des exemples concrets.
- **Variez les messages.** Assurez-vous d'avoir, pour chaque thème, plusieurs contenus dont la présentation et la formulation varient.
- **Impliquez les apprenants.** Un contenu et des exercices interactifs améliorent la rétention.
- **Forcez-les à réfléchir.** Les exercices doivent tester la façon dont les apprenants appliquent les connaissances acquises.
- **Mesurez les résultats.** Évaluez les apprenants au départ et suivez constamment leurs progrès.

Utilisation de contenus et supports variés pour que la formation reste intéressante

D'après la « règle de sept », un prospect doit voir sept fois le message d'un annonceur pour passer à l'action. Il en va de même pour les formations.

Quelle que soit la solution de formation et de sensibilisation à la sécurité informatique que vous utilisez, vos leçons doivent être présentées au moyen de différents canaux et activités. Voici quelques exemples d'activités et de canaux que vous pouvez utiliser.

ACTIVITÉS	CANAUX
Simulations d'attaque (phishing, USB, SMS, etc.)	Outils de formation et de sensibilisation à la sécurité informatique
Évaluations des connaissances	Outils de formation et de sensibilisation à la sécurité ou outil d'enquête
Identification et surveillance des VAP	Threat intelligence / passerelle de messagerie
Formation assistée par ordinateur	Modules de formation et de sensibilisation à la sécurité via une plate-forme en ligne ou un autre système de gestion des formations (LMS)
Campagnes de sensibilisation	Posters, vidéos, podcasts, webinaires, conférenciers, infographies
Exercices de formation et de sensibilisation virtuels ou en personne	Déjeuners de présentation, webinaires, stands lors d'événements de l'entreprise, tours de parole lors d'événements de l'entreprise, formation en personne, escape games (jeux d'évasion)
Concours / jeux	Reconnaissance d'un changement de comportement positif via un canal d'entreprise existant (par exemple, newsletter ou wiki)
Informations de sensibilisation à la sécurité informatique	Wiki d'entreprise, intranet ou calendrier d'entreprise partagé
Mise à jour des informations de sensibilisation à la sécurité informatique	Newsletter d'entreprise, application de communication (par exemple, Microsoft Teams et Slack) ou intégration aux communications d'un autre département interne
Feedback utilisateur sur le programme de formation et de sensibilisation à la sécurité informatique	Outil d'enquête ou boîte email partagée
Signalement de phishing par les utilisateurs	Module d'extension du client de messagerie ou boîte email de signalement d'abus



Lorsque les utilisateurs ont une piètre opinion de la formation de sensibilisation à la sécurité informatique de leur entreprise, ils peuvent y être indifférents, voire s'y opposer.

Implication d'autres départements internes et de personnes occupant des postes clés

Les responsables des services marketing, de sécurité informatique et RH ainsi que d'autres dirigeants clés peuvent jouer un rôle majeur dans votre programme. Faites appel à leur expertise pour soutenir et améliorer votre approche, votre contenu et votre mode de présentation.

Voici quelques suggestions quant à l'assistance que peuvent apporter d'autres départements internes :

- Le service de **sécurité informatique** peut recommander du contenu adapté aux règles de l'entreprise (par exemple, les règles en matière de mots de passe). Il peut également identifier les utilisateurs nécessitant une formation supplémentaire s'il constate qu'ils sont davantage ciblés lors de cyberattaques ou gèrent des informations sensibles.
- Le service **marketing** peut collaborer à la conception de supports de sensibilisation à la sécurité informatique et d'autres contenus afin qu'ils soient conformes aux éléments de marque de votre entreprise.
- Le service **RH** peut apporter des conseils sur la dynamique organisationnelle et fournir des informations utiles sur la collaboration avec les dirigeants et les responsables des différents pôles d'activité.
- Le **RSSI** (ou d'autres chefs de service ou membres de la direction) peuvent apporter leur soutien et insister sur l'importance du programme.

La carotte ou le bâton : orientation du comportement des utilisateurs afin de l'améliorer

Lorsque les utilisateurs ont une piètre opinion de la formation de sensibilisation à la sécurité informatique de leur entreprise, ils peuvent y être indifférents, voire s'y opposer. Jusqu'ici, nous avons présenté les étapes susceptibles de créer les conditions requises pour la mise sur pied d'un programme bien accepté et bien pensé. Lorsqu'il s'agit de privilégier la carotte ou le bâton en matière de formation, la plupart de nos clients préfèrent généralement la première approche.

Mais de temps à autre, la résistance des utilisateurs peut exiger le recours à la seconde. Dans ces cas très rares, la modélisation des conséquences peut favoriser le respect de la politique de formation. Même s'il s'agit d'une solution de dernier recours, voici quelques types de modèles de conséquences utilisés par nos clients :

- Application du principe des « trois infractions » – les utilisateurs qui cliquent sur trois emails lors de simulations d'attaques de phishing sont tenus d'avoir un entretien avec leur supérieur hiérarchique ou se voient temporairement privés de leur accès réseau ou de leurs privilèges d'accès
- Conséquences diverses telles que rapports RH, diminutions de salaire, des primes ou des avantages et, dans de rares cas, licenciement

Une bonne pratique consiste à se concentrer sur des mesures incitatives positives et à n'utiliser la modélisation des conséquences qu'en dernier recours. Nos clients constatent que l'utilisation excessive de sanctions nuit à l'engagement des utilisateurs vis-à-vis du programme. Cela étant, si votre entreprise appartient à un secteur très réglementé ou sensible, l'usage du bâton s'avère parfois nécessaire.

SECTION 4

Le rôle essentiel des données

Une fois votre programme de sensibilisation à la sécurité informatique approuvé, vous êtes sans doute pressé de commencer les simulations d'attaques de phishing et de dispenser des formations avancées aux utilisateurs.

Il est toutefois important de commencer par un plan stratégique. Pour maximiser les bénéfices (diminution des risques posés par les utilisateurs) et minimiser les coûts (le temps consenti par les utilisateurs), les premières étapes devraient être les suivantes : offrir des connaissances de base, comprendre les vulnérabilités des utilisateurs et donner la priorité aux formations réellement nécessaires.

Mise en place des bases

En tant qu'expert en sécurité, votre premier instinct est sans doute de simuler des attaques de phishing avancées ou de former les utilisateurs à la détection des principales menaces ciblant votre entreprise. Si cette attitude est assez logique, elle n'aura pas l'impact escompté si vos utilisateurs ne possèdent pas les connaissances de base requises.

Dans notre rapport State of the Phish 2020, nous avons constaté que de nombreux collaborateurs en entreprise sont incapables de définir des termes tels que le phishing et le ransomware.

Qu'est-ce que le **PHISHING ?**

Réponses correctes	Réponses incorrectes	Je ne sais pas
61 %	24 %	15 %

- Seuls 49 % des collaborateurs aux États-Unis ont répondu correctement.
- Les collaborateurs allemands sont ceux qui ont été les plus nombreux à reconnaître ce terme (66 %).

Qu'est-ce que le **RANSOMWARE ?**

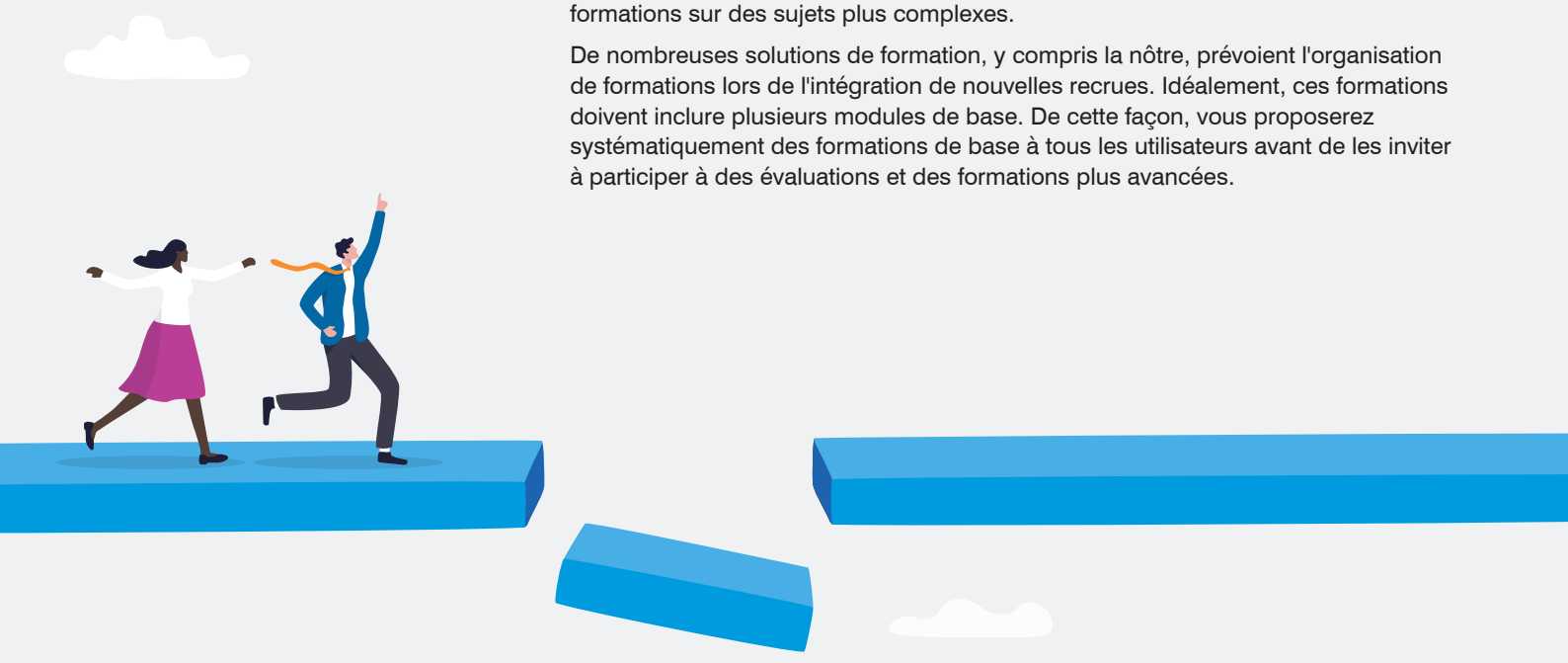
Réponses correctes	Réponses incorrectes	Je ne sais pas
31 %	31 %	38 %

- L'année dernière, 45 % des collaborateurs, tous pays confondus, ont répondu correctement à cette question. Cette diminution de la sensibilisation pourrait s'expliquer par la forte baisse du nombre d'attaques de ransomwares observée en 2018, le sujet étant dès lors moins abordé dans les communications entre les utilisateurs et les équipes de sécurité.

Source : State of the Phish 2020

Ces lacunes sont la raison même pour laquelle nous recommandons vivement des formations sur des thèmes élémentaires, notamment les principes fondamentaux de la sécurité ou le phishing, avant d'évaluer les utilisateurs ou de leur donner des formations sur des sujets plus complexes.

De nombreuses solutions de formation, y compris la nôtre, prévoient l'organisation de formations lors de l'intégration de nouvelles recrues. Idéalement, ces formations doivent inclure plusieurs modules de base. De cette façon, vous proposerez systématiquement des formations de base à tous les utilisateurs avant de les inviter à participer à des évaluations et des formations plus avancées.



Identification des utilisateurs vulnérables et des VAP

Sur la base du modèle VAP décrit dans l'introduction, votre programme doit accorder une attention prioritaire aux utilisateurs qui posent un risque élevé pour les raisons suivantes :

- Ils sont particulièrement vulnérables aux tactiques des cybercriminels.
- Ils sont plus souvent ciblés lors des attaques.
- Ils disposent de privilèges d'accès à des données, systèmes ou ressources de valeur.

(Consultez la section « Modèle de mesure et de limitation du risque utilisateur centré sur les personnes » à la page 3.)

Mesure des vulnérabilités, des attaques et des privilèges

En ce qui concerne les vulnérabilités, les simulations d'attaques de phishing et les tests d'évaluation des connaissances représentent des outils très précieux. Ils vous aident à identifier les utilisateurs nécessitant une formation complémentaire, les tactiques auxquelles ils sont vulnérables et les domaines à couvrir.

En ce qui concerne les attaques, pour identifier les utilisateurs les plus ciblés, les tactiques utilisées et le type de cybercriminels, vous avez besoin des informations fournies par la solution de threat intelligence de votre équipe de sécurité. Ces VAP sont identifiés au moyen de notre « Attack Index », un score composite prenant en compte les facteurs suivants :

- **Type de cybercriminel.** Ce facteur se réfère au niveau de sophistication du pirate et, par voie de conséquence, au niveau de risque pour l'entreprise. Par exemple, l'auteur d'une attaque à la solde d'un État recevra un score beaucoup plus élevé qu'un cybercriminel de petite envergure.
- **Type de ciblage.** Cet attribut définit la précision avec laquelle la cible est choisie. La menace a-t-elle touché un seul utilisateur ou avait-elle une portée mondiale ? Visait-elle un utilisateur, une entreprise, un secteur ou une zone géographique en particulier ? Ou s'agissait-il d'une campagne à large spectre, qui a touché la moitié de la planète ? Plus la menace est ciblée, plus son score est élevé.
- **Type de menace.** Cet attribut prend en considération le type de malware impliqué dans l'attaque. Dans la plupart des cas, le malware employé nous renseigne sur la gravité de la menace ou l'ampleur des efforts déployés pour l'exécuter. Un cheval de Troie d'accès à distance (RAT), par exemple, obtiendra un score plus élevé qu'une tentative de phishing d'identifiants de connexion générique ciblant les particuliers.

En ce qui concerne les privilèges, les entreprises peuvent commencer par recenser tous les éléments potentiellement de valeur auxquels les utilisateurs ont accès (données, autorité financière, relations clés, etc.).

La position de l'utilisateur dans l'organigramme de l'entreprise est bien entendu un facteur à prendre en compte lors de l'évaluation des privilèges. Ce n'est cependant pas le seul facteur – et bien souvent, il est loin d'être le plus important. Une assistante de direction peut constituer une cible plus intéressante qu'un manager dans un objectif d'espionnage industriel, car elle a accès à l'emploi du temps du PDG. De la même façon, une infirmière travaillant à l'hôpital et ayant accès aux dossiers des patients peut constituer, pour les usurpateurs d'identité, une cible plus judicieuse que le directeur général.

La quantification du risque utilisateur conformément au modèle VAP vous permet de cibler votre programme de formation et de limiter plus rapidement le risque.

Pratiques en matière de mots de passe

utilisent un gestionnaire de mots de passe

effectuent une rotation parmi 5 à 10 mots de passe différents

saisissent manuellement un mot de passe différent à chaque connexion

utilisent le même ou les deux mêmes mots de passe pour tous leurs comptes

Source : State of the Phish 2020

Utilisation des données VAP au-delà de la formation

La quantification du risque utilisateur conformément au modèle VAP vous permet de cibler votre programme de formation et de limiter plus rapidement le risque. Elle vous offre également un contexte permettant de comprendre les raisons pour lesquelles les cybercriminels ciblent ces utilisateurs. Grâce à ces renseignements, vous pouvez surveiller plus attentivement ces utilisateurs et ceux attachés à des fonctions similaires, et déployer des contrôles adaptatifs, par exemple en isolant les activités de navigation ou en renforçant l'authentification, lorsque nécessaire.

Lorsque vous combinez ces informations avec la threat intelligence (par exemple, les données fournies par un outil tel que Proofpoint Targeted Attack Protection (TAP)), vous pouvez déterminer avec une plus grande précision si les utilisateurs sont ciblés par du contenu malveillant.

S'il est utile de savoir si les utilisateurs cliquent sur les emails lors des simulations d'attaques de phishing, il est encore plus important de déterminer s'ils cliquent sur du contenu malveillant réel, même si ce clic est bloqué. Ces données permettent de mettre en évidence les risques et failles potentiels.

Au-delà du phishing : maîtrise d'autres thèmes de sécurité sensibles

Le phishing est l'un des thèmes les plus abordés lors des formations de sensibilisation à la sécurité informatique. Mais si vous limitez votre programme aux seules menaces propagées par email, vous risquez de passer à côté d'autres problèmes de sécurité majeurs.

Envisagez de procéder à une évaluation globale des connaissances de vos utilisateurs afin de mieux cerner leur compréhension des grands thèmes de cybersécurité et des consignes et règles de votre entreprise.

Notre rapport State of the Phish 2020 a révélé plusieurs comportements à risque. En voici quelques exemples :

- 45 % des employés reconnaissent utiliser les mêmes mots de passe pour plusieurs comptes.
- Seuls 49 % d'entre eux protègent le réseau Wi-Fi de leur domicile.
- 26 % sont convaincus que se connecter à un réseau Wi-Fi gratuit dans un lieu de confiance, tel qu'un café ou un aéroport, est sans danger.
- 17 % ignorent si les réseaux publics de ces endroits sont sûrs.

De tels comportements exposent votre entreprise à des risques sérieux. Pour les limiter, il est bon de diversifier votre programme afin qu'il aborde ces sujets ainsi que d'autres vulnérabilités potentielles.

Lorsque vous abordez ces thèmes, utilisez des exemples marquants et des témoignages réels. Des détails concrets et pertinents aident les utilisateurs à mieux comprendre le mode opératoire des cybercriminels et les raisons d'y prêter attention.

Mise en place d'un programme agile

Chaque entreprise est associée à un paysage des menaces, des utilisateurs et une culture de sensibilisation à la sécurité informatique qui lui sont propres. Et si la planification est importante, l'agilité l'est tout autant.

Un programme agile s'adapte au changement de circonstances et attribue les formations aux bonnes personnes, au bon moment. Il permet aussi de s'assurer que le contenu est complet, efficace et performant. Enfin, il contribue à réduire le risque utilisateur en exploitant au mieux les quelques heures que la plupart des entreprises peuvent consacrer chaque année aux formations de sensibilisation à la sécurité informatique.

Les programmes les plus performants basent les exercices donnés lors des formations sur des menaces réelles et potentielles. Adaptez votre programme en fonction de l'évolution des circonstances. La vie est imprévisible et un changement soudain peut créer de nouveaux risques utilisateur et lacunes.

Voici quelques exemples de situations dans lesquelles vous devrez modifier vos plans en fonction des besoins ou des vulnérabilités récemment mises au jour :

- Vos évaluations de phishing montrent que vos utilisateurs comprennent les attaques distribuant des liens malveillants mais qu'ils éprouvent des difficultés à repérer les attaques impliquant des pièces jointes.
- Votre entreprise est prise pour cible par un nombre croissant d'attaques BEC (Business Email Compromise).
- L'équipe responsable de la sécurité de la messagerie remarque que des cybercriminels utilisent une marque spécifique de leurre de phishing ou un type d'attaque particulier.
- Lors de vos évaluations des connaissances, vous constatez qu'un département interne rencontre des difficultés avec un thème de sécurité majeur.

Automatisation des formations de suivi

L'automatisation de ces formations peut améliorer encore l'agilité de votre programme. Par exemple, nos clients utilisent la fonctionnalité d'inscription automatique de notre solution pour attribuer automatiquement des sessions de formation selon les résultats obtenus par les utilisateurs lors des simulations d'attaques et des évaluations des connaissances. Cette fonctionnalité attribue des formations aux utilisateurs qui en ont le plus besoin mais ne les oblige pas à la suivre à ce moment-là.

Le suivi automatisé est un bon moyen d'adapter les formations aux vulnérabilités et lacunes réellement identifiées, plutôt que d'opter pour une approche globale qui attribue la même formation à tous les utilisateurs. Une formation ciblée permet aux utilisateurs de gagner du temps et favorise l'adoption du programme par tous les acteurs concernés.

Possibilité « d'exemption » des utilisateurs

Un autre moyen d'adapter la formation consiste à offrir aux utilisateurs la possibilité d'être « exemptés » dès lors qu'ils démontrent qu'ils maîtrisent les concepts de cybersécurité et adoptent des comportements appropriés. Si les utilisateurs ont suivi les formations de base, rejettent (ou signalent) systématiquement les simulations d'attaques de phishing et obtiennent de bons résultats aux évaluations des connaissances, ils n'ont sans doute pas besoin de suivre toutes les formations.

Cette possibilité d'exemption peut inciter les utilisateurs à mieux percevoir les formations et à participer plus consciencieusement aux évaluations.

SECTION 5

Les indicateurs qui comptent : mesure du succès du programme

Si vous avez mis en place un programme de sensibilisation à la sécurité informatique, le taux de clics, également appelé taux d'échec, vous est sans doute familier. C'est la toute première statistique dont parlent les clients qui cherchent à évaluer l'efficacité de leur programme. Il s'agit donc d'un indicateur de première importance.

Taux de signalement

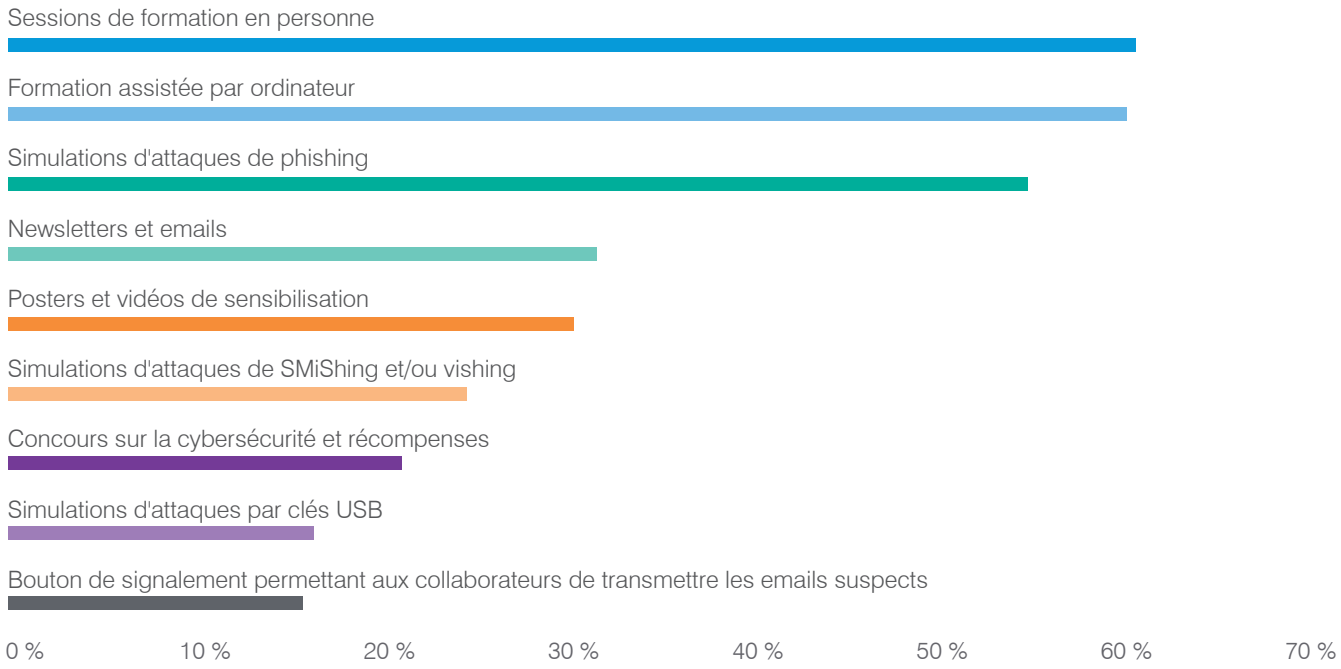
Mais ce n'est pas le seul indicateur auquel vous devez faire attention. Le taux de signalement des emails malveillants (réels et simulés) par les utilisateurs peut fournir des indications précieuses.

Les modules de signalement d'emails intégrés aux clients de messagerie permettent aux utilisateurs d'avertir facilement leur équipe de sécurité de la réception d'emails suspects. Ces outils peuvent également calculer le nombre d'utilisateurs qui, après avoir reçu un email de simulation d'attaque de phishing, le signalent, un indicateur connu comme le taux de signalement.

Malheureusement, seulement 15 % des entreprises utilisent ces outils dans le cadre de leur programme de sensibilisation à la sécurité informatique, selon notre rapport State of the Phish 2020.

Nos données font apparaître de plus grandes variations au niveau du taux de signalement que des taux de clics, ce qui laisse penser que le taux de signalement est, globalement, un meilleur indicateur de changement du comportement.

Outils utilisés par les entreprises dans leurs programmes*



* Plusieurs réponses étaient admises.

Source : State of the Phish 2020

Niveaux de connaissance

Le niveau de connaissance constitue une autre source d'informations précieuse. Les taux de clics et de signalement permettent de mesurer la résilience des utilisateurs aux attaques de phishing. En revanche, les évaluations des connaissances permettent de savoir dans quelle mesure ils comprennent d'autres thèmes, notamment la confidentialité des données, les mots de passe et la sécurité pour mobiles.

Par exemple, des entreprises ou départements internes très réglementés peuvent exiger des formations spécifiques. Il est essentiel de bien comprendre les niveaux de connaissance des utilisateurs et de déterminer s'ils sont en baisse ou en hausse.

Taux de clics et de signalement de référence

Si vous envoyez un email de simulation d'attaque de phishing, quel taux de clics est considéré comme « bon » ? La réponse dépend essentiellement de deux facteurs :

- Le niveau de difficulté et de ciblage de la simulation d'attaque de phishing
- L'expérience de vos utilisateurs

En règle générale, des taux de clics (ou taux d'échec) inférieurs à 5 % sont considérés comme de bons résultats. L'écart (supérieur ou inférieur) par rapport au taux d'échec moyen enregistré dans un large éventail d'entreprises constitue toutefois une mesure plus précise.

Proofpoint, à l'instar de nombreux autres éditeurs, fournit le taux d'échec moyen de différents modèles de simulation d'attaque de phishing. Comme l'illustre la capture d'écran ci-dessous, un taux d'échec de 5 % reflète un résultat inférieur à la moyenne pour certains modèles.

En règle générale, des taux de clics (ou taux d'échec) inférieurs à 5 % sont considérés comme de bons résultats.

Comparaison des taux d'échec moyens de notre produit ThreatSim® *(en vert)*

Jump in this quick meeting	Corporate	8%
FREE GDPR Readiness Tools - Targets Legal or HR	Commercial	3%
College Admissions Help	Consumer	2%
Online dating - Message waiting	Proofpoint - Consumer	5%

C'est pourquoi la comparaison des résultats de vos utilisateurs à ces taux d'échec moyens offre une indication plus intéressante de leur sensibilisation au phishing. Les taux d'échec moyens peuvent changer au fil du temps, compte tenu de l'adoption de certains modèles par un nombre croissant d'entreprises.

En ce qui concerne les taux de signalement (le nombre d'utilisateurs qui identifient un email de simulation d'attaque de phishing comme suspect et le signalent), visez un taux de 70 %. Plusieurs de nos clients ont enregistré des taux de signalement supérieurs à 80 %, ainsi qu'un faible taux d'échec.

Mesure de l'impact

Les indicateurs de mesure de la sensibilisation à la sécurité informatique sont importants et devraient être facilement accessibles depuis votre programme de sensibilisation à la sécurité. Mais le véritable objectif d'un tel programme est la réduction du risque utilisateur.

À cet égard, les indicateurs externes peuvent vous aider à évaluer et démontrer la valeur de votre programme. Voici quelques indicateurs clés :

- Nombre d'infections de malwares et mesures correctives appliquées aux machines des utilisateurs
- Temps et ressources consacrés à la gestion de la boîte email de signalement d'abus
- Nombre d'attaques de phishing couronnées de succès
- Heures d'interruption pour les utilisateurs

Ces indicateurs peuvent également vous aider à conserver l'adhésion des principales parties prenantes à votre programme. Un de nos clients a réduit ses dépenses liées aux effectifs de 345 000 dollars en utilisant un composant de notre solution CLEAR (Closed-Loop Email Analysis and Response). (Pour en savoir plus, lisez le rapport de Forrester « The Total Economic Impact Of Proofpoint Advanced Email Protection » (L'impact économique total de la solution Proofpoint de protection avancée de la messagerie).)

Un de nos clients a réduit ses dépenses liées aux effectifs de

345 000 $

en utilisant un composant de notre solution CLEAR.

Utilisation des données pour orienter la conversation

De nombreux indicateurs utilisés pour évaluer les formations de sensibilisation à la sécurité informatique, notamment les taux d'échec, de clics et autres, peuvent avoir une connotation négative et souligner les erreurs plutôt que les points positifs. D'autres indicateurs, tels que les taux de signalement et les niveaux de connaissance, mettent en avant les comportements positifs plutôt que négatifs. En outre, ils mettent davantage en évidence les performances des utilisateurs en tant que ligne de défense contre les attaques ciblées actuelles.

Utilisez ces données en guise de témoignage de la contribution des utilisateurs au renforcement de la sécurité de votre entreprise. Imaginons qu'un utilisateur signale un message réellement malveillant et que votre équipe de réponse aux incidents l'élimine avant qu'il compromette votre entreprise. De tels témoignages peuvent vous aider à promouvoir votre programme en interne et renforcer la sécurité de votre entreprise.

SECTION 6

Au-delà de la formation : comment instaurer une culture de la sécurité informatique

Près de 99 % des entreprises déclarent proposer une formation de sensibilisation au phishing à leurs collaborateurs[2]. Cependant, 43 % d'entre elles n'offrent cette formation qu'à une partie de leur personnel. Il n'est dès lors pas étonnant que le phishing reste la menace la plus susceptible de provoquer une compromission de données.

Comment donc améliorer la situation ? En instaurant une culture de la sécurité informatique systématique, durable et personnalisée, qui couvre l'ensemble de l'entreprise, des utilisateurs et des activités numériques.

Cette approche nécessite un investissement concerté en temps, en efforts et en ressources, ainsi qu'un soutien à l'échelle de l'entreprise. Mais les bénéfices sont inestimables. Une culture de la sécurité informatique solidement ancrée peut améliorer le niveau de protection, la conformité et les résultats opérationnels de votre entreprise. Elle peut même renforcer la confiance et la productivité de vos collaborateurs.

2 Proofpoint, « State of the Phish 2022 », février 2022.

Qu'est-ce qu'une culture de la sécurité informatique ?

Selon Keman Huang et Keri Pearlson, chercheurs au MIT, une culture de la sécurité informatique représente « les croyances, valeurs et attitudes qui motivent les utilisateurs à protéger et défendre leur entreprise contre les cyberattaques[3] ».

Autrement dit, tous les collaborateurs, sans exception, sont des agents actifs de la défense des données, systèmes et ressources de l'entreprise.

Pour instaurer une culture de la sécurité informatique, vous devez modifier les croyances de vos collaborateurs en la matière. Une culture de la sécurité informatique doit faire partie intégrante de la culture de base de votre entreprise. Elle doit inspirer et perdurer.

Qu'est-ce qui façonne une culture ?

La culture de la cybersécurité comprend trois facteurs qui se recoupent :

- **Responsabilité à l'égard de la cybersécurité.** Les collaborateurs se sentent, individuellement et collectivement, responsables de leurs actes en faveur de la prévention des incidents de sécurité.
- **Compréhension de l'importance de la cybersécurité.** Les collaborateurs sont conscients que les cybermenaces constituent un risque majeur pour la réussite de l'entreprise et peuvent les toucher personnellement.
- **Capacité d'agir.** Les collaborateurs gagnent en autonomie grâce à leurs connaissances en matière de cybersécurité, à la maîtrise des règles de sécurité et à la certitude que l'entreprise les soutiendra s'ils commettent involontairement une erreur de sécurité.

Caractéristiques d'une culture robuste de la sécurité informatique

Une culture robuste de la sécurité informatique présente les caractéristiques suivantes :

- **Globalité et continuité.** Une culture de la sécurité informatique ne doit pas se limiter à des formations ou à des simulations de phishing occasionnelles. L'objectif est de nourrir un climat de confiance avec tous les collaborateurs pour renforcer leur implication et améliorer leurs comportements en matière de sécurité informatique. Plusieurs méthodes peuvent être mises en œuvre à cette fin. Une culture de la sécurité informatique favorise l'apprentissage et la sensibilisation grâce à des contenus pertinents et personnalisés et à un suivi de l'évolution du paysage des menaces. Les utilisateurs reçoivent des emails et autres rappels pour les aider à comprendre les raisons de leur participation au programme et les bénéfices qu'ils peuvent en retirer dans leur vie professionnelle et privée. Ils sont encouragés à signaler en toute confiance les événements numériques suspects.
- **Interlocuteurs privilégiés transversaux.** Ces interlocuteurs assurent la transmission entre l'équipe de direction et les utilisateurs finaux, en passant par les responsables intermédiaires. Outre l'équipe de direction, les « promoteurs » peuvent être issus d'autres services, notamment la sécurité, les technologies de l'information, les ressources humaines, la conformité et l'audit, le marketing et les relations publiques[4].
- **Création et soutien des attentes.** Cela implique d'élaborer et d'appliquer des règles de sécurité informatique à l'appui des normes culturelles.

3 Keman Huang and Keri Pearlson (MIT), « For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture » (Ériger un modèle de la culture de la cybersécurité organisationnelle pour pallier les failles de la technologie), janvier 2019.

4 SANS Institute, « 2021 Security Awareness Report: Managing Human Cyber Risk » (Rapport 2021 sur la sensibilisation à la sécurité informatique : gérer le cyberrisque humain), novembre 2021.

Les avantages

Une culture solide de sensibilisation à la sécurité informatique peut faire progresser la mission de l'entreprise et offrir des avantages significatifs et mesurables. En voici quelques exemples :

Amélioration de l'agilité et de la résilience

Une culture de la sécurité informatique encourage les utilisateurs à détecter les menaces potentielles. Elle permet également aux équipes de sécurité d'intervenir et de neutraliser les menaces plus rapidement. L'agilité et la résilience sont renforcées lorsque des utilisateurs motivés, impliqués et solidaires les uns envers les autres parviennent à créer un effet de réseau. Les bénéfices se répercutent dans toute l'entreprise.

Réduction des risques pour l'entreprise

Nous vivons dans une ère de changement, avec le passage au télétravail ou à une approche hybride, la migration vers le cloud et l'utilisation accrue des terminaux personnels. Les risques s'en trouvent multipliés. Une culture solide de la sécurité informatique permet de rassurer les dirigeants, qui pourront ainsi se consacrer à d'autres activités.

Conformité sans peine

Le respect des réglementations officielles, des normes sectorielles et des règles de sécurité internes est facilité, avec pour résultat une réduction du risque d'amendes et autres sanctions.

Avantage concurrentiel

Les clients et les partenaires choisiront votre entreprise plutôt que vos concurrents s'ils se sentent plus en sécurité. Promouvez la sécurité en tant que valeur fondamentale.

Obstacles courants

Les entreprises dépensent des millions dans des outils, des services et du personnel de sécurité. Pourtant, nombreuses sont celles qui, en dépit de ces investissements, négligent le principal facteur de risque : les collaborateurs.

Prendre en compte le facteur humain est la première mesure de sécurité à mettre en place. C'est aussi la plus compliquée. Les programmes de sensibilisation peuvent s'avérer déstabilisants et être une source de distraction. Certains collaborateurs ont le sentiment que ces programmes les empêchent de faire correctement leur travail. Nombreux sont ceux qui rechignent à effectuer certaines tâches supplémentaires, comme signaler les emails suspects ou participer à des webinaires de formation. De plus, l'équipe technique et les ressources humaines peuvent hésiter à mettre en place une culture de la sécurité informatique, faute de moyens pour l'instaurer et l'entretenir.

Principaux défis :

- Faire accepter l'idée à la direction
- Quantifier de façon convaincante le retour sur investissement
- Convaincre les utilisateurs des bénéfices de la formation et de la sensibilisation à la sécurité informatique et les amener à y prendre activement part
- Modifier le comportement des utilisateurs

De la théorie à la pratique avec le cadre ACE

La motivation est essentielle pour mettre en place une culture robuste de la sécurité informatique, fondée sur trois ingrédients principaux. Le premier est l'autonomie. Chaque utilisateur doit bénéficier d'une formation personnalisée et auto-gérée. Le deuxième est la maîtrise. Vous devez mettre à la disposition des utilisateurs les outils et le temps dont ils ont besoin pour progresser et asseoir leurs connaissances et leurs compétences en matière de cybersécurité. Le dernier ingrédient est la finalité. Vos utilisateurs doivent avoir le sentiment de prendre part à une mission qui dépasse leur propre fonction.

Utilisation du cadre ACE

L'instauration d'une culture durable de la sécurité informatique comporte trois étapes. Il s'agit d'un processus continu, que nous appelons le cadre ACE.

A Analyser la vulnérabilité des utilisateurs

Chaque entreprise est unique, avec ses propres risques et priorités en matière de sécurité.

Posez-vous les questions suivantes :

- Quel est le niveau de connaissance de mes utilisateurs ?
- Qui est ciblé ? Par quels types d'attaques ?
- Que feraient ces utilisateurs s'ils étaient confrontés à des menaces ?
- Quelles sont leurs croyances ? Que pensent-ils de la cybersécurité ?

Ces questions et d'autres vous aideront à identifier vos vulnérabilités.

C Changer les comportements

L'instauration d'une culture de la sécurité informatique est un processus continu, et non un événement ponctuel. Adoptez une approche globale.

Cela implique de communiquer régulièrement avec vos collaborateurs par le biais de multiples canaux de communication, notamment des newsletters régulières, des blogs internes et des mises à jour sur les menaces et les vecteurs d'attaque les plus récents.

Variez et personnalisez les contenus. Chaque utilisateur est unique, et réagit et apprend différemment. Pensez à rappeler en permanence l'importance de la sécurité de façon positive.

E Évaluer les progrès jusqu'à la réussite

Partagez des mesures qui montrent les progrès réalisés, les améliorations continues et le retour sur investissement. Ces mesures quantifiables permettront de justifier votre investissement et de démontrer la valeur d'une culture de la sécurité informatique à la direction et à l'entreprise tout entière.

Ne laissez pas passer la moindre occasion. Après une attaque, montrez comment une culture plus solide de la sécurité informatique aurait permis de réduire le temps, les coûts et les efforts nécessaires à sa résolution ou aidé l'entreprise à l'éviter complètement.

Différents moyens permettent de mesurer le niveau de sensibilisation à la sécurité informatique de votre entreprise et, partant, d'évaluer le changement de comportement des utilisateurs induit par votre culture de la sécurité.

Par exemple :

- Taux de clics des utilisateurs les plus vulnérables
- Taux de signalement des simulations d'attaques de phishing
- La précision avec laquelle vos utilisateurs peuvent identifier les menaces réelles

Pourquoi est-ce important ?

L'instauration d'une culture robuste de la sécurité informatique offre des avantages à l'ensemble de vos utilisateurs, de l'équipe de direction aux utilisateurs finaux, en passant par l'équipe de sécurité et les responsables.

Il n'existe pas de modèle universel. Chaque entreprise est différente et a des besoins uniques. Certaines de ces différences tiennent aux activités de l'entreprise, d'autres au secteur. Chaque culture de la sécurité informatique est déterminée par un ensemble de facteurs internes et externes.

L'instauration d'un programme durable approuvé à tous les niveaux permet d'ancrer la sensibilisation à la sécurité informatique dans les valeurs fondamentales de l'entreprise. Une véritable culture de la sécurité ne se limite pas à une session de formation ponctuelle. C'est un état d'esprit qui guide les activités au quotidien et les actions individuelles.

Cette section est une introduction générale à l'instauration d'une culture de la sécurité informatique.

Pour en savoir plus sur les cultures de la sécurité informatique et le cadre ACE, téléchargez notre eBook *Au-delà de la formation de sensibilisation – L'importance d'instaurer une culture de la sécurité informatique durable.*

SECTION 7

Conclusions et recommandations

Votre programme de formation et de sensibilisation à la sécurité informatique doit avoir pour objectif le développement de comportements essentiels à la mission de votre entreprise. Pour y parvenir, la meilleure solution consiste à combiner des formations générales et ciblées qui responsabilisent les utilisateurs au moyen de conseils pratiques.

Si vous n'avez pas encore adopté une approche centrée sur les personnes en matière de sensibilisation à la sécurité informatique, n'attendez plus. Voici les cinq piliers d'un programme efficace et performant :

Développement d'un programme centré sur les personnes

Chaque collaborateur de l'entreprise peut être une cible. De même, chaque collaborateur peut à tout moment contribuer à la sécurité ou la mettre à mal.

Les formations de sensibilisation des utilisateurs constituent l'une des principales mesures à prendre pour sécuriser votre entreprise. En apprenant à vos utilisateurs à identifier, rejeter et signaler les tentatives de phishing, vous pouvez ériger une dernière ligne de défense robuste contre les cybermenaces les plus dangereuses d'aujourd'hui.

Planification de votre déploiement

Chaque entreprise est unique et chaque programme sera donc différent. Néanmoins, comme expliqué dans la section 2, tous doivent inclure les éléments suivants :

- Définition des besoins de formation
- Identification des utilisateurs présentant des besoins de formation spécifiques
- Définition des activités
- Élaboration et gestion des calendriers
- Communication et test des premières étapes
- Définition de la fréquence et du timing des activités du programme

Le succès de votre programme va dépendre du soin que vous mettez à le concevoir et d'une bonne planification.

Engagement des utilisateurs

Il est essentiel de préserver l'intérêt des utilisateurs si vous voulez que votre programme soit un succès. Malheureusement, même les programmes les mieux intentionnés peuvent devenir pénibles s'ils n'offrent pas une expérience attrayante et pertinente aux utilisateurs.

Les programmes les plus performants :

- Utilisent un label pour que les utilisateurs se rendent compte de leur intérêt
- S'appuient sur des principes d'apprentissage éprouvés pour changer les comportements
- Renforcent la formation par toute une série de contenus et de supports
- Font appel à des « promoteurs » dans toute l'entreprise dans un but de soutien et d'amélioration
- Guident les utilisateurs grâce à un juste équilibre entre incentives et conséquences

Utilisation des données pour identifier les utilisateurs vulnérables, formation ciblée et agilité

Les premières étapes doivent consister à dispenser des connaissances de base, comprendre les vulnérabilités des utilisateurs et centrer vos formations sur les lacunes identifiées. À cet égard, les simulations d'attaques de phishing et les évaluations des connaissances peuvent vous fournir des informations précieuses sur les aspects de la sécurité nécessitant une formation. Les informations de threat intelligence peuvent également vous éclairer sur les attaques auxquelles vos utilisateurs sont confrontés afin que vous puissiez aligner le contenu de vos formations sur les menaces réelles. Par ailleurs, en identifiant les utilisateurs qui ont accès aux données les plus sensibles de l'entreprise, vous pouvez adapter les formations et imposer des contrôles de sécurité supplémentaires aux utilisateurs à privilèges.

L'automatisation des formations de suivi et les possibilités d'exemption pour les utilisateurs avertis et présentant peu de risques vous permettent de rester agile et d'adapter votre programme.

Mesure du succès du programme à l'aide d'indicateurs internes et externes

Les taux de clics (ou taux d'échec) pour les simulations d'attaques de phishing sont importants. Mais les taux de signalement d'emails sont probablement une indication plus fiable de la résilience de vos utilisateurs face aux attaques.

Les évaluations des connaissances permettent de déterminer dans quelle mesure ils comprennent d'autres thèmes de cybersécurité.

Enfin, les indicateurs externes, comme les infections de malwares et les interruptions, peuvent aider à démontrer l'impact et la valeur de votre programme.

Ils peuvent également vous aider à conserver l'adhésion des principales parties prenantes à votre programme. Utilisez ces données pour mettre en avant la façon dont les utilisateurs contribuent au renforcement de la sécurité de votre entreprise. Vous pourrez ainsi promouvoir plus efficacement le programme en interne, mais aussi améliorer la culture de sécurité informatique de votre entreprise.

En savoir plus

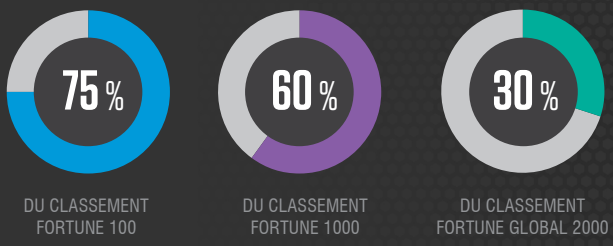
Pour en savoir plus sur les connaissances en cybersécurité de vos utilisateurs, leurs forces et leurs faiblesses et déterminer comment favoriser un changement de comportement, faites appel à notre évaluation gratuite des risques, sur la page proofpoint.com/fr/people-risk-assessment.

Pourquoi Proofpoint

Chaque jour, nous analysons plus de :

2,6 Mrd D'EMAILS	**49 Mrd** D'URL	**1,9 Mrd** DE PIÈCES JOINTES
1,7 Mrd DE MESSAGES MOBILES	**430 Mio** DE DOMAINES WEB	**143 000** COMPTES DE RÉSEAUX SOCIAUX

Nos solutions ont été adoptées par plus de :



8 000 GRANDES ENTREPRISES

200 000 PETITES ENTREPRISES

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0504-001-03-02 10/22