# Le guide complet de la formation à la sensibilisation à la sécurité

# 2021

# Contenu

Introduction

# Comment les attaques ciblées sur l'homme vont évoluer en 2021

**La pandémie de Covid-19 a posé de nombreux problèmes de sécurité. Les entreprises du monde entier se sont adaptées au travail à domicile et à la distanciation sociale, tout en faisant face aux nouvelles menaces que représentent les cybercriminels qui exploitent la peur et la curiosité. Alors même que les entreprises ont fait face à ces défis, les cybermenaces traditionnelles ont été plus répandues que jamais, ce qui a rendu la cybersécurité essentielle pour toutes les entreprises**

**Parmi les principales cybermenaces, les logiciels malveillants restent un danger important. L'épidémie de WannaCry de 2017, qui a coûté aux entreprises du monde entier jusqu'à 4 milliards de dollars, est encore dans les mémoires et d'autres nouvelles souches de logiciels malveillants sont découvertes chaque jour.**

Le phishing a également connu une recrudescence ces dernières années, avec de nombreuses nouvelles escroqueries inventées pour profiter d'entreprises peu méfiantes. Une seule variante, l'escroquerie par e-mail de la CEO Fraud, a coûté aux seules entreprises britanniques 14,8 millions de livres sterling en 2018.

Le personnel travaillant à domicile n'est pas sous la surveillance directe des équipes de support informatique, et a souvent du mal à faire face aux cyber-menaces et à protéger de manière appropriée les informations de l'entreprise.

L'absence de mise à jour des logiciels et des systèmes d'exploitation, l'envoi de données sur des réseaux non sécurisés et la dépendance croissante à l'égard du courrier électronique et de la messagerie en ligne ont rendu les employés beaucoup plus vulnérables aux menaces allant des logiciels malveillants au phishing.

Si les solutions techniques telles que les filtres antispam et les systèmes de gestion des appareils mobiles sont importantes pour la protection des utilisateurs finaux, compte tenu du nombre de menaces et de la multitude de systèmes et de communications par lesquels le personnel travaille, le seul facteur de risque en commun qui doit être pris en compte pour améliorer fondamentalement la sécurité est le rôle de l'erreur humaine.

# Pourquoi l'erreur humaine est la menace numéro 1 pour la sécurité de votre entreprise

Presque toutes les brèches de données réussies ont une variable en commun : l'erreur humaine. L'erreur humaine peut se manifester de multiples façons : de l'échec de l'installation des mises à jour de sécurité des logiciels à temps à la faiblesse des mots de passe et à l'abandon d'informations sensibles dans des e-mails de phishing.

Même si les logiciels modernes de lutte contre les logiciels malveillants et de détection des menaces sont devenus plus sophistiqués, les cybercriminels savent que l'efficacité des mesures de sécurité techniques dépend de leur utilisation correcte par les humains.

Si un cybercriminel parvient à deviner le mot de passe d'un portail d'entreprise en ligne, ou utilise l'ingénierie sociale pour amener un employé à effectuer un paiement sur un compte bancaire contrôlé par le cybercriminel, il n'y a rien que les solutions techniques puissent faire pour arrêter cette intrusion.

En 2014, IBM a mené une étude sur les brèches de données qui se sont produites chez des milliers de ses clients dans plus de 130 pays. Cette étude était la plus vaste étude sur les causes des brèches de données qui avait été réalisée à ce moment-là, mais ses résultats ont depuis été corroborés par des études similaires.

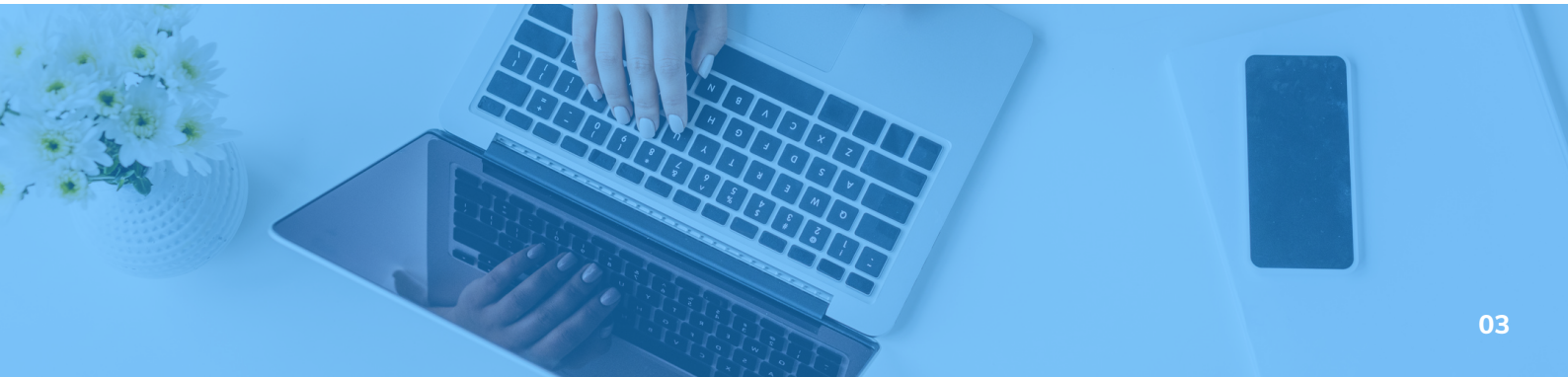
L'une des principales conclusions de l'étude d'IBM était que l'erreur humaine était une cause majeure de 95% des brèches de données

En d'autres termes, si l'erreur humaine n'avait pas été un facteur, il est probable que 19 des 20 brèches analysées dans l'étude ne se seraient pas produites du tout.

> " L'erreur *humaine a été un facteur décisif dans 95 % des brèches* "

L'erreur humaine jouant un rôle si important dans les brèches de données, il est essentiel d'y remédier pour réduire les chances que votre entreprise soit ciblée avec succès. Elle vous permet également de protéger votre entreprise contre un éventail de menaces beaucoup plus large que ne le pourrait une solution technique à elle seule - et peut potentiellement donner à votre personnel les moyens de rechercher activement et de signaler les nouvelles menaces auxquelles il pourrait être confronté.

La réduction de l'erreur humaine doit être la clé de la cybersécurité des entreprises en 2021 - et dans la prochaine section, nous examinerons les meilleurs moyens d'y parvenir.



## Quand l'erreur humaine se produit-elle ?

Deux facteurs doivent être présents pour que l'erreur humaine se manifeste : l'opportunité et la décision. L'opportunité signifie qu'il y a une situation où l'on permet à un humain de faire une erreur : par exemple, laisser les utilisateurs finaux gérer les mises à jour de logiciels plutôt que de forcer les mises à jour de sécurité par la gestion des correctifs. La décision est l'action de l'individu : dans ce cas, l'absence d'action dans l'installation des mises à jour de sécurité lorsqu'elles sont disponibles.

Un effort global d'atténuation comprend à la fois la réduction des possibilités d'erreur et l'amélioration des décisions prises par les utilisateurs finaux. Il est essentiel de prendre des mesures dans ces deux domaines pour garantir que l'erreur humaine soit traitée de manière approfondie.

Dans le cas des correctifs, par exemple, une mesure technique telle que l'introduction de la gestion des correctifs peut réduire au minimum les possibilités d'erreur humaine dans la plupart des cas - mais il est toujours essentiel de tenir compte des situations où les solutions techniques sont temporairement caduques, ou si une nouvelle situation telle qu'une politique BYOD où les utilisateurs sont autorisés à utiliser leurs propres appareils sans gestion des correctifs est introduite.

Dans d'autres cas, comme celui des e-mails de phishing, les mesures techniques telles que les filtres anti-spam et les logiciels de détection des brèches ont un effet très limité pour réduire les possibilités d'erreur face à une attaque ciblée. Dans ces cas, la seule manière efficace d'atténuer l'erreur humaine est d'apprendre aux utilisateurs finaux à mieux discerner la situation.

*"Deux facteurs doivent être présents pour que l'erreur humaine se manifeste : opportunité et decision"*

# Comment les employés peuvent-ils prendre des décisions de sécurité plus sûres au quotidien ?

## 1 Comprendre

**L'utilisateur doit être conscient qu'il se trouve dans une situation où la sécurité est potentiellement en jeu. Sans le réaliser, l'utilisateur peut même ne pas se rendre compte qu'il prend une décision par son inaction.**

## 2 Renforcement

**L'utilisateur doit savoir quelle est la bonne marche à suivre. Cela ne signifie pas nécessairement qu'il doit se rendre totalement compte de la menace, mais il suffit souvent de signaler la situation à une personne du service informatique ou de sécurité qui peut y jeter un oeil.**

## 3 Education

**L'utilisateur doit savoir pourquoi la sécurité est importante, afin qu'il comprenne l'importance de ne pas ignorer les procédures de sécurité et qu'il soit conscient des implications potentielles d'une brèche.**

## 4 Se débarasser de la fainéantise

**Des problèmes tels que la faiblesse de la sécurité des mots de passe et l'incapacité à corriger les logiciels persistent dans les organisations du monde entier, bien que de nombreux utilisateurs comprennent pourquoi ces problèmes sont critiques pour la sécurité. La raison pour laquelle aucune mesure n'est prise malgré la connaissance de ces problèmes est due à ce que nous appelons la fainéantise. Avoir un mot de passe unique et fort demande plus de temps pour le créer et plus d'efforts pour s'en souvenir qu'un mot de passe court, faible ou réutilisé.**

**Bien que l'utilisateur puisse connaître les mesures de sécurité appropriées, cette "fainéantise" causée par la création d'un mot de passe fort est souvent assez forte pour qu'il tombe dans le panneau. Cette situation est aggravée par le fait que, bien que de nombreux utilisateurs prennent les mesures appropriées dans des circonstances optimales, les situations de travail urgentes et chargées, ainsi que le stress, peuvent rendre les mesures de sécurité encore plus pénibles pour les utilisateurs.**

Les utilisateurs finaux doivent sentir que la contrainte causée par le respect des meilleures pratiques de sécurité est moindre que la satisfaction obtenue en ne le faisant pas. Les mesures techniques telles que les gestionnaires de mots de passe sont essentielles à cet égard, car elles facilitent grandement l'action en matière de sécurité : si les employés ne doivent pas créer ou mémoriser leurs propres mots de passe, ils n'ont aucune raison de ne pas utiliser des mots de passe sûrs.

Simultanément, il faut abaisser le seuil d'exécution de l'action correcte par un changement culturel. Cela signifie qu'il faut placer la sécurité au premier plan de la prise de décision et veiller à ce que les utilisateurs n'aient jamais l'impression de "perdre du temps" en prenant les précautions de sécurité appropriées.

Une formation efficace à la sensibilisation à la sécurité ne traite pas d'un seul de ces facteurs, mais des quatre. Cela signifie qu'il faut identifier les situations dans lesquelles les données ou les systèmes pourraient être compromis, comprendre les meilleures pratiques, connaître les conséquences potentielles des brèches, et enfin contribuer à faire passer un changement culturel pour créer un environnement où les considérations de sécurité sont toujours prises en compte dans la prise de décision.

Sensibilisation à la sécurité à domicile

# Garantir la sécurité du personnel lorsqu'il travaille à domicile

**La réponse mondiale à la pandémie de Covid-19 a entraîné de nombreux changements sur les lieux de travail. Le changement qui a eu l'impact le plus significatif sur la sécurité a été la transformation de nombreuses entreprises qui ont vu la plupart ou la totalité de leur personnel passer au travail à domicile dans un court laps de temps, ce qui a entraîné un risque accru pour de nombreux utilisateurs finaux de succomber aux menaces en ligne.**

**Les employés qui n'avaient pas l'habitude de travailler à domicile avant la pandémie ont rapidement découvert certains des problèmes qu'elle entraînerait : devoir s'occuper d'enfants et des animaux domestiques, faire face à une mauvaise connexion à Internet et supporter tous les autres problèmes qui peuvent survenir à la maison. Au milieu de tous ces nouveaux changements dans l'environnement de travail, la sécurité fini trop souvent au bas de la liste des priorités des utilisateurs.**

Les utilisateurs finaux qui travaillent à domicile ne sont pas sous la surveillance du service d'assistance informatique et peuvent être confrontés à des problèmes techniques simples. De plus, des tâches de sécurité essentielles comme la mise à jour des logiciels et des systèmes d'exploitation, la mise à jour du micrologiciel des routeurs et la sécurisation du réseau, ont soudainement été confiées aux utilisateurs finaux.

Il n'est pas étonnant que les cybercriminels n'aient pas tardé à exploiter les circonstances de la pandémie pour mettre au point de nouvelles formes d'escroquerie et de cybercriminalité.

*Au milieu de tous ces nouveaux changements dans l'environnement de travail, la sécurité est trop souvent reléguée au bas de la liste des priorités des utilisateurs.*

# Comment aborder la sécurité lorsque les utilisateurs finaux sont chez eux

L'équipe de soutien informatique ne peut pas se rendre au domicile de chaque utilisateur final, c'est pourquoi il est essentiel de s'assurer que, en plus de disposer du bon équipement, les utilisateurs finaux sont conscients de leurs responsabilités individuelles dans le maintien de la sécurité. Les utilisateurs finaux doivent savoir qu'il leur incombe de veiller à ce qu'ils n'accèdent aux informations et aux réseaux de l'entreprise que sur des appareils et des réseaux à jour et sécurisés.

La formation de sensibilisation à la sécurité est essentielle pour que les utilisateurs finaux sachent comment assurer la sécurité chez eux. Il est préférable de diviser la formation en petits éléments assimilables, car cela permet de s'assurer que les utilisateurs ne sont pas submergés d'informations. La formation doit également avoir lieu régulièrement - au minimum une fois par mois - pour s'assurer que les connaissances clés sont conservées et que les utilisateurs n'oublient pas la sécurité dès qu'un nouveau projet de travail vient bouleverser la liste des priorités. Enfin, il est important de tester les utilisateurs finaux

Il convient de préciser qu'il ne s'agit pas de juger ou de pénaliser les utilisateurs qui ont du mal à suivre leur formation, mais plutôt d'identifier les principales lacunes en matière de sécurité dans l'ensemble du personnel et de les combler avant qu'elles ne puissent être exploitées par des cybercriminels.

*"La formation à la sécurité est essentielle pour que les utilisateurs finaux sachent comment assurer la sécurité"*

Formation à l'ancienne VS formation moderne

# Comment choisir le meilleur format pour la formation de sensibilisation à la sécurité

**La formation de sensibilisation à la sécurité n'est pas la même pour tous. La manière dont la formation est dispensée, structurée et présentée aura un effet majeur sur son efficacité à améliorer véritablement les résultats en matière de sécurité dans votre organisation. Dans cette section, nous examinerons la meilleure façon de dispenser une formation de sensibilisation à la sécurité à vos utilisateurs finaux.**

**La formation de sensibilisation à la sécurité consistait auparavant à faire assister les utilisateurs finaux à une session annuelle comprenant des heures de conférences et de diaporamas. L'idée était que les utilisateurs se souviennent de quelque chose de ce qu'ils ont vu et entendu - et dans le pire des cas, la case "éduquer les utilisateurs" pouvait au moins être cochée. Mais dans quelle mesure cela a-t-il réellement amélioré les résultats en matière de sécurité ? Cela n'a pas fonctionné et tout le monde a détesté cette idée.**

## Pourquoi une session par an ne marche jamais

Plusieurs raisons expliquent pourquoi ce type de formation annuelle basée sur des conférences n'est pas efficace.

La première est que dans une session de formation annuelle il y aura tout simplement trop d'informations à la fois pour qu'un employé puisse les assimiler et s'en souvenir.

Même si les utilisateurs reçoivent du matériel pédagogique à emporter avec eux ou reçoivent des rappels occasionnels, il y a de fortes chances que la plupart du matériel de la session de formation passe par une oreille et ressorte par l'autre - oublié en quelques instants.

Les conférences et les diaporamas ne sont tout simplement pas des formats stimulants dont les utilisateurs finaux peuvent tirer des leçons. Ils ne parviennent pas à susciter l'intérêt des employés comme le font les vidéos et les contenus interactifs, et sont trop souvent remplis d'informations inutiles qui ne sont pas pertinentes pour chaque utilisateur final.

Les diapositives remplies à ras bord de petits textes sont sûres de faire s'endormir n'importe quel employé au milieu de la session.

La dernière raison, la plus importante, pour laquelle la formation traditionnelle n'est pas efficace est qu'elle ne fait pas appel à l'apprentissage par la répétition. S'il s'écoule un an entre deux sessions d'apprentissage, les utilisateurs ne se souviendront tout simplement pas de ce qu'ils ont appris - et la sensibilisation aux questions de sécurité en général s'effondrera dans les jours et les semaines qui suivent la formation. La sécurité ne peut pas être une chose ponctuelle, mais doit être assurée toute l'année pour être efficace.

## Comment rendre la formation moderne vraiment efficace

### Divisier le contenu

Il y a une quantité limitée d'informations qu'une personne peut absorber à la fois. Afin de ne pas submerger les utilisateurs finaux, la formation doit être divisée en segments, chacun ayant son propre message clair et simple, présenté de manière facilement assimilable.

### Apprentissage en continu

La division du matériel didactique permet également de rendre l'apprentissage facilement continu, plutôt que ponctuel, et d'envoyer des cours régulièrement tout au long de l'année, ce qui contribue à maintenir la sensibilisation à la sécurité dans l'esprit des utilisateurs finaux et à améliorer la rétention de l'apprentissage.

### Contenu pertinent

Lorsqu'un utilisateur final reçoit des informations qu'il estime ne pas être pertinentes pour lui, il commence rapidement à se désintéresser et à prêter moins d'attention. Le matériel didactique doit non seulement éviter le jargon et les termes techniques, mais aussi être conçu en tenant compte des situations réelles que l'utilisateur final pourrait rencontrer.

La formation à la sensibilisation à la sécurité s'est de plus en plus orientée vers des solutions logicielles en ligne. La formation en ligne offre certains avantages immédiats par rapport aux méthodes traditionnelles, mais elle n'est pas nécessairement la réponse ultime à la sensibilisation à la sécurité, à moins qu'elle n'apporte des résultats dans certains domaines essentiels pour améliorer véritablement la sécurité.

### Faire de la cybersécurité une partie même de la culture de l'entreprise

La formation doit s'inscrire dans une culture d'entreprise où la sécurité est toujours prise en compt et où les utilisateurs sont encouragés à faire part de leurs préoccupations et à poser des questions.

### Conseils pratiques

Il est essentiel que les employés quittent la formation en ayant à l'esprit des étapes concrètes qu'ils peuvent mettre en pratique immédiatement dans leurs activités professionnelles quotidiennes. Donner aux employés la possibilité de mettre leur formation à l'épreuve immédiatement contribue également à développer leur mémoire - et peut être réalisé à l'aide d'outils tels que la simulation de phishing.

### Vidéo et contenu interactif

Les vidéos et les contenus interactifs sont parfaits pour attirer les utilisateurs qui préfèrent un autre type d'expérience d'apprentissage. De nombreuses personnes apprennent en faisant, en répondant à des questions ou en participant d'une autre manière.

### Mesurer l'impact

Il est essentiel qu'après les sessions de formation, les utilisateurs soient testés sur ce qu'ils ont appris. Cela vous permet de savoir que les utilisateurs s'en vont après avoir appris quelque chose - mais cela facilite également le processus d'apprentissage des utilisateurs, car ils se souviennent des informations qu'ils viennent d'apprendre de leur propre mémoire.

Construire une culture de la sécurité

# Comment intégrer la sécurité dans la culture quotidienne du personnel

**La formation de sensibilisation à la sécurité ne sera pas efficace pour améliorer les résultats en matière de sécurité si elle n'est pas accompagnée d'un changement culturel. Une formation complète apprendra aux utilisateurs finaux à reconnaître les situations où la sécurité est menacée et à les traiter de manière appropriée - mais ces connaissances ne seront pas mises en pratique si l'utilisateur n'a pas le sentiment que la sécurité est valorisée dans sa culture.**

**Avec le nombre croissant de menaces présentes, ainsi que la complexité croissante des services aux entreprises et l'accès aux données et aux systèmes à partir d'appareils mobiles, il est impossible de savoir où pourrait apparaître la prochaine menace ou fuite accidentelle pour votre entreprise.**

C'est pourquoi la sécurité ne doit pas consister à s'assurer que vos utilisateurs finaux choisissent des mots de passe forts ou suivent d'autres étapes spécifiques, mais plutôt à leur permettre d'être des gardiens actifs de votre entreprise, de ses systèmes, de ses dispositifs et de ses données.

*"La formation de sensibilisation à la sécurité ne sera pas efficace pour améliorer les résultats en matière de sécurité si elle n'est pas accompagnée d'un changement culturel."*

# Comment construire une culture de la sécurité

### Obtenir un soutien de niveau C

Le changement culturel et les valeurs de l'entreprise doivent venir d'en haut. Les cadres supérieurs ont un rôle important à jouer en mettant l'accent sur le rôle de la sécurité dans l'entreprise - mais il est essentiel qu'ils développent, plutôt que de dicter, la nouvelle culture.

Cela signifie qu'il faut encourager les employés à jouer un rôle actif en leur demandant de faire part de leurs préoccupations concernant leur propre rôle, et les inciter à poser des questions et à s'engager dans les questions de sécurité. De cette façon, les utilisateurs ont le sentiment d'être impliqués dans le processus de sécurité et commencent à réfléchir activement aux considérations de sécurité dans leur propre rôle.

### Le moins d'accès possible

Si le principe du moins de privilège possible est souvent considéré comme une mesure technique - limitant chaque utilisateur aux seuls privilèges dont il a besoin pour ses fonctions spécifiques - il devrait également être directement intégré dans la culture d'entreprise.

Cela signifie qu'il faut encourager les utilisateurs à signaler activement les cas où ils ont accès à plus de données ou de systèmes qu'ils n'en ont besoin, ce qui contribue à limiter les possibilités de violation.

### Sécurité physique

En termes de mesures physiques, des éléments comme les affiches peuvent être utiles pour instaurer une culture de la sécurité, et contiennent également des rappels utiles sur des sujets tels que la force des mots de passe.

Il est cependant important de se rappeler que le simple fait de coller une affiche sur un mur n'apportera rien en soi, mais qu'elle doit être utilisée comme point de départ pour la discussion, ou servir de complément au matériel de formation dans lequel les utilisateurs sont déjà impliqués.

Thèmes essentiels de formation pour 2021

# Quels sont les thèmes de formation essentiels pour 2021 ?

**Bien que chaque organisation et chaque fonction aient des exigences différentes, il existe certains domaines essentiels qu'il convient de faire connaître à chaque utilisateur final.**

## Topics phares pour 2021 :

1. Techniques de phishing
2. Ingénierie sociale
3. Securité à domicile
4. Utilisation sécurisée d'internet et du courrier électronique
5. Travailler à domicile
6. Sécurité des appareils mobiles
7. Mot de passe et authentification
8. Sécurité du cloud
9. Wi-Fi public
10. Sécurité physique
11. Supports amovibles
12. Utilisation sécurisée des réseaux sociaux

### #1. Techniques de phishing

Le phishing reste une menace énorme. L'une des raisons pour lesquelles le phishing est si populaire parmi les cybercriminels est qu'il peut être facilement personnalisé pour tirer parti de n'importe quel événement ou circonstance - comme la pandémie de Covid-19 - afin de cibler les utilisateurs avec de nouvelles arnaques. Les escroqueries basées sur des modèles offrant des informations aux victimes sont plus populaires que jamais, tandis que les attaques de spear-phishing qui ciblent les utilisateurs individuels et les entreprises restent les plus dangereuses.

Les utilisateurs finaux sont les plus susceptibles de recevoir des e-mails de phishing qui créent un sentiment d'urgence ou offrent quelque chose de précieux à l'utilisateur. Il est essentiel de former les utilisateurs finaux à vérifier qu'ils peuvent faire confiance à l'expéditeur d'un e-mail avant de cliquer sur des liens ou de renoncer à des informations. Bien qu'il soit impossible pour les utilisateurs d'attraper tous les e-mails de phishing, une sensibilisation à la sécurité combinée à des filtres anti-spam permet de limiter au maximum la portée potentielle des e-mails de phishing.

### #2. Ingénierie sociale

Le phishing n'est qu'un des nombreux types d'attaques d'ingénierie sociale. Les attaques d'ingénierie sociale physiques et téléphoniques sont également utilisées par les criminels pour accéder à des locaux sécurisés et à des données sensibles.

Il est essentiel que les employés soient formés aux différents types d'attaques d'ingénierie sociale - des menaces par téléphone aux menaces en personne - et qu'ils comprennent comment traiter correctement tout contrevenant potentiel.

### #3. Sécurité à domicile

Le travail à domicile a été placé au premier plan de la sécurité des utilisateurs finaux en 2020, les entreprises du monde entier ayant encouragé leur personnel à passer au travail à distance. La rapidité de ce transfert a fait que de nombreux utilisateurs ont été mal équipés en outils et connaissances pour effectuer leur travail en toute sécurité.

Il est essentiel de former tous les employés travaillant à domicile à la manière dont ils peuvent s'assurer que les données et le réseau de l'entreprise ne sont pas compromis par un accès à distance. La mise à jour des logiciels, la protection des réseaux Wi-Fi et l'utilisation d'outils de sécurité tels que les VPN pour garantir un accès sécurisé sont devenus une partie essentielle de la formation des utilisateurs finaux.

### #4. Utilisation sécurisée d'Internet et du courrier électronique

En 2021, il est rare qu'un employé n'utilise pas internet ou ses e-mails au travail. Si la pandémie a rendu les entreprises plus dépendantes que jamais d'internet, l'utilisation de l'internet comporte également des risques pour la sécurité. Les utilisateurs peuvent installer par inadvertance des logiciels malveillants, divulguer des données, renoncer à leur accréditation pour les e-mails de phishing ou se laisser prendre à l'une des nombreuses autres attaques dont les cybercriminels les prennent pour cible.

La formation devrait également comporter des conseils pratiques, par exemple en informant les utilisateurs sur la différence entre les champs cc et bcc, et sur la signification du symbole de cryptage HTTPS sur les sites web.

### #5. Travailler à domicile

En 2021, le travail à distance va être plus populaire que jamais. Si la pandémie a donné un coup de pouce au travail à domicile dans de nombreuses entreprises, il est probable qu'elle se poursuivra au-delà de la pandémie. Les employés ont commencé à s'habituer au travail à domicile, et les entreprises en réalisent les avantages.

Travailler à distance comporte également des risques. Les ordinateurs portables, les téléphones mobiles, les tablettes et autres appareils peuvent constituer une grave menace pour la sécurité s'ils sont perdus ou volés. Si les employés stockent ou accèdent aux données de l'entreprise à partir de leurs appareils mobiles, toutes ces données deviennent vulnérables si un appareil tombe entre de mauvaises mains. Lors de la formation des utilisateurs au télétravail sécurisé, il convient de s'attacher à les aider à identifier les points où les systèmes ou les données pourraient être compromis - et les mesures qu'ils peuvent prendre pour atténuer ces risques.

### #6. Sécurité des appareils mobiles

L'utilisation des appareils mobiles dans les entreprises a connu une croissance rapide et, en 2021, cette tendance devrait se généraliser encore plus qu'auparavant. Les appareils mobiles tels que les ordinateurs portables, les téléphones mobiles et les tablettes permettent aux employés de travailler à domicile, dans les cafés, en voyage ou à peu près n'importe où, ce qui leur offre une certaine souplesse, tant pour eux-mêmes que pour l'entreprise. Aussi pratiques que soient les appareils mobiles, ils comportent des risques dont les utilisateurs doivent être informés.

### #7. Mots de passe et authentification

Les mots de passe restent un casse-tête majeur pour les entreprises, les employés et les clients. Les humains ne sont tout simplement pas conçus pour se souvenir de phrases longues et complexes - surtout pas de dizaines d'entre elles. Cela signifie que les employés sont constamment tentés de choisir la facilité et de les rendre faciles à retenir, surtout lorsqu'ils doivent partager l'accès aux applications et aux services avec leurs collègues.

La majorité des utilisateurs finaux savent pourquoi la sécurité des mots de passe est importante, et ont une idée générale de ce qui fait un mot de passe fort. La formation sur les mots de passe et l'authentification doit se concentrer sur des conseils pratiques sur la manière de maintenir la sécurité des mots de passe sans rendre la vie plus difficile à vos utilisateurs finaux. Cela signifie qu'il faut encourager l'utilisation de gestionnaires de mots de passe (si votre entreprise le permet), demander aux employés d'activer l'authentification à deux facteurs pour tous les services et systèmes ayant accès à des données sensibles, et leur apprendre comment créer un mot de passe qui soit à la fois raisonnablement complexe et facile à retenir.

### #8. Sécurité du Cloud

Ces dernières années, les services et les données des entreprises se sont de plus en plus déplacés vers le cloud. En 2021, cette tendance atteint son point culminant, de nombreuses opérations commerciales étant menées entièrement à l'aide d'outils et de services basés sur le web. Si le nuage offre une grande flexibilité aux entreprises, il est essentiel que les utilisateurs sachent comment l'utiliser et y accéder en toute sécurité.

Des mots de passe et une authentification solides, ainsi que la sécurité du courrier électronique, revêtent une importance supplémentaire lorsque votre entreprise utilise des services du cloud.

### #9. Wi-Fi public

Comme les utilisateurs travaillent de plus en plus souvent en déplacement, il y a de fortes chances qu'ils se connectent à des services, des réseaux ou des données d'entreprise à partir de points d'accès Wi-Fi publics. Le Wi-Fi public est très pratique pour le travail mobile, mais il comporte également des risques pour la sécurité.

Il est important d'apprendre aux utilisateurs finaux que leurs données pourraient potentiellement être interceptées sur les réseaux Wi-Fi publics. Si vous permettez à vos utilisateurs finaux d'accéder aux données ou aux services de l'entreprise par l'intermédiaire des réseaux Wi-Fi publics, vous devez les équiper d'un logiciel de réseau privé virtuel et leur apprendre à l'utiliser de manière sécurisée.

### #10. Sécurité physique

Même si les menaces de cybersécurité se multiplient, il est essentiel que la sécurité physique ne soit pas négligée. Il ne sert à rien de protéger les données avec des mots de passe forts et une authentification à plusieurs facteurs si une personne non autorisée peut simplement entrer dans le bureau et prendre une copie papier d'un document sensible directement dans le bac de l'imprimante.

Lors de la formation des utilisateurs finaux en matière de sécurité physique, il est essentiel de mettre l'accent sur l'identification et l'atténuation des menaces liées aux activités quotidiennes de chaque utilisateur final. Si votre entreprise est basée dans un bureau, chaque employé va passer par la porte du bureau - le tailgating est donc un exemple de menace à la sécurité qui concerne tous les employés. Les utilisateurs finaux doivent être formés à réfléchir activement aux zones et aux documents qui sont sécurisés, et à veiller à ce qu'ils soient toujours verrouillés de manière sûre ou à ce qu'on en rende compte lorsqu'ils ne sont pas utilisés.

### #11. Supports amovibles

Même si le partage de fichiers et les services de collaboration en ligne sur internet sont devenus plus populaires, les supports amovibles sont encore largement utilisés dans les entreprises. Aussi utiles soient-ils, les dispositifs amovibles présentent de nombreux risques : ils se perdent ou se volent facilement, ce qui peut compromettre les données, ou peuvent être remplacés par des dispositifs contenant des logiciels malveillants. Une arnaque courante consiste à laisser une clé USB infectée par un virus dans un parking, en attendant d'être ramassée et insérée dans un ordinateur de l'entreprise par un employé sans méfiance. En outre, de nombreux utilisateurs ignorent que les dispositifs de stockage ne sont pas les seuls à présenter un risque : même de simples câbles USB ou de chargement peuvent être modifiés par un cybercriminel pour contenir un logiciel malveillant.

L'éducation des utilisateurs finaux à l'utilisation sécurisée des supports amovibles se résume à la responsabilisation. Il faut faire comprendre aux utilisateurs qu'ils doivent assumer la responsabilité des appareils qui sont sous leur contrôle - et qu'ils ne doivent pas brancher sur un ordinateur des appareils qui ont disparu, mais les signaler à l'équipe informatique ou au personnel de sécurité.

### #12. Utilisation sécurisée des réseaux sociaux

Les employés - et les entreprises - passent une partie croissante de leur journée sur les réseaux sociaux. Il est toutefois essentiel de s'assurer que la sécurité de l'entreprise ne sera pas compromise par une utilisation imprudente des réseaux sociaux.

La formation aux réseaux sociaux devrait être axée sur la sensibilisation des utilisateurs au fait que ce qu'ils partagent peut être accessible à tous sur Internet - et que même les petits détails provenant du bureau peuvent être cruciaux pour les agresseurs. Par exemple, un innocent égoïste du bureau pourrait montrer un tableau blanc en arrière-plan avec des informations commerciales sensibles, ou même les coordonnées d'un client.