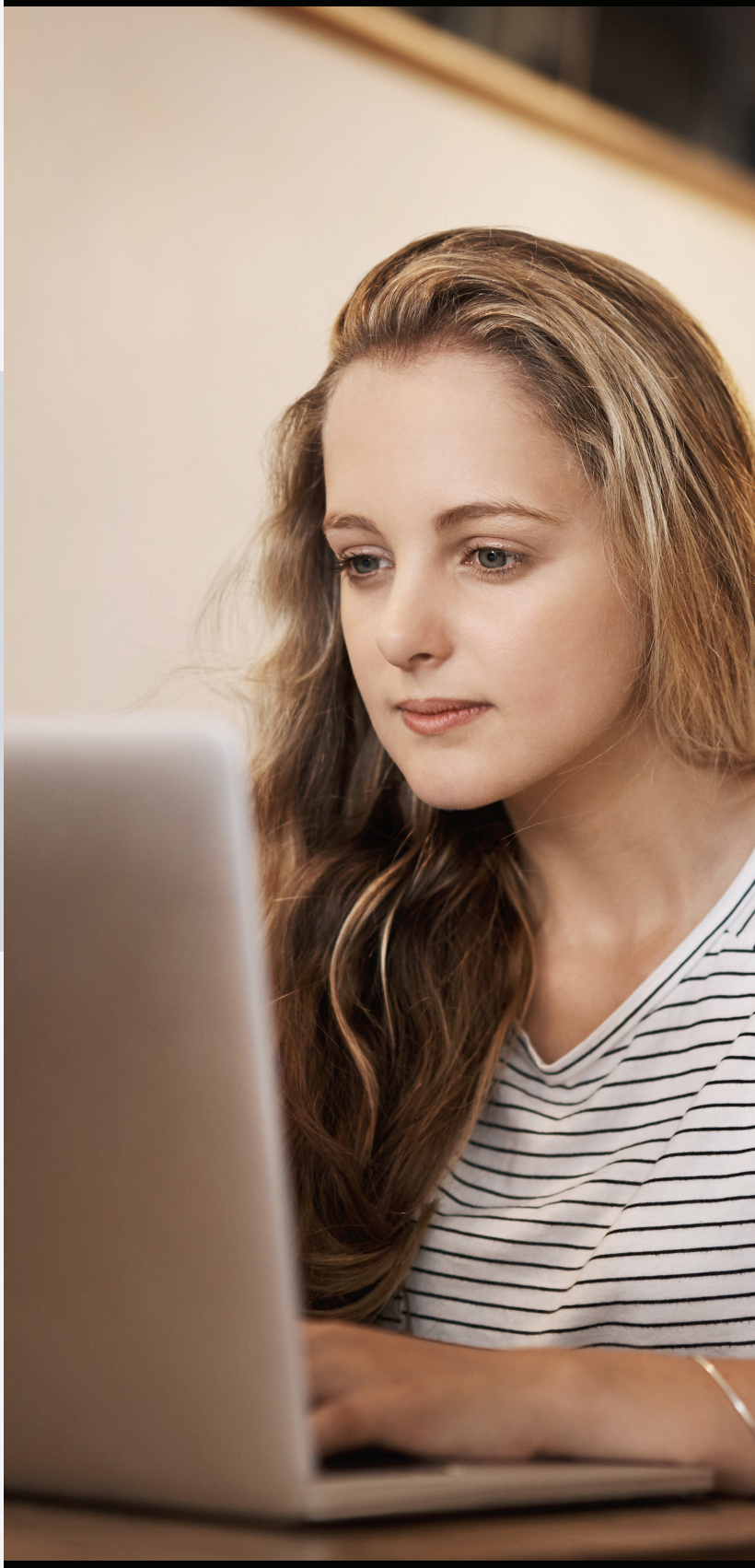
Consolider la première ligne de défense et le maillon le plus faible : les personnes.

IBM Security



Pour un employé, la meilleure façon de protéger une organisation contre les menaces de cybersécurité consisterait à ne jamais ouvrir de courrier électronique. Il serait préférable de former les employés.

Sensibilisation et services de formation à la sécurité IBM Security

IBM Security propose un développement de programme complet et une adaptation continue de la sensibilisation à la sécurité et de l'éducation à l'hameçonnage, ceci afin de promouvoir une culture de sensibilisation au risque. Nous fournissons un programme de sensibilisation continue sur mesure pour votre entreprise.

Le hameçonnage demeure un vecteur de menace principal et nos services aident les employés à mieux se préparer contre ce danger et contre l'ingénierie sociale. Nous formons vos employés au moyen de l'apprentissage en ligne, de la ludification, et de simulations de hameçonnage et ingénierie sociale. Nos conseillers chevronnés fournissent une personnalisation de plateforme, des méthodes de formation sur mesure, des métriques, et une gestion des rapports et du programme.

Commencez dès aujourd'hui

Découvrez les avantages d'un programme de sensibilisation et formation à la sécurité.

Contactez les services IBM Security à : **ibm.biz/BdqYUF.**

IBM

Un programme complet de sensibilisation et formation à la sécurité peut contribuer à atténuer le risque organisationnel.

Cinq étapes du développement du programme.

1. Définir

- **Définir les objectifs du programme**
- **Définir le public cible (champ d'application)**
- **Définir les KPI**
- **Définir les exigences liées au programme et à la conformité**

2. Établir

- **Établir un cadre de sensibilisation à la cybersécurité**
- **Établir un plan de sensibilisation**
- **Établir des artefacts, des guides de formation**
- **Obtenir le soutien du leadership**

3. Évaluer

- **Évaluer l'état actuel des connaissances sur la sécurité des informations**
- **Évaluer l'état actuel de la compréhension des employés sur leur rôle et leur capacité vis-à-vis de la sécurité des informations**

4. Déployer

- **Réaliser des intégrations et une personnalisation**
- **Diriger des formations, des campagnes, des questionnaires et enquêtes d'opinion**
- **Formation par ordinateur, activation du client**

5. Mesurer

- **Faire un suivi et mesurer l'efficacité du programme**
- **Faire des rapports sur les évaluations et la formation**
- **Produire des résultats comparables avec des campagnes en guise de référence**

Valeur

- Une équipe dédiée pour un programme continu
- Personnalisé et sur mesure selon les besoins des clients
- Aide à réduire la dépendance aux compétences internes
- Un programme formel de sensibilisation et formation à la sécurité
- Une gestion continue du programme

Bénéfices

- Aide à réduire le nombre d'incidents
- Aide à minimiser le coût total lié aux incidents
- Une mise en œuvre cohérente dans toute l'organisation
- Relie en direct à des tests de hameçonnage avec une formation ciblée
- Aide à améliorer la sensibilisation à la sécurité et un changement de comportement