FeelAgile

Sensibilisation à la sécurité de l'information

Cette sensibilisation vise à renforcer la vigilance des collaborateurs face aux cybermenaces en les dotant des connaissances nécessaires pour protéger les informations sensibles de l'entreprise. Elle aborde des sujets clés tels que le phishing, la sécurité du cloud et l'utilisation de l'IA, afin de promouvoir des pratiques sécuritaires au quotidien.

Durée : 2h - 16 modules vidéos au choix - *Format E-learning, accessible à tout moment selon les disponibilités des collaborateurs.*

Public concerné

- Cette sensibilisation est destinée à l'ensemble des collaborateurs de l'entreprise, quel que soit leur niveau hiérarchique ou leur fonction.
- Elle vise à renforcer la culture de la sécurité de l'information au sein de toutes les équipes, en impliquant chaque employé dans la protection des données sensibles de l'organisation.

Prérequis

- Aucun prérequis. Cette sensibilisation s'adresse à tous les collaborateurs, quel que soit leur poste ou leur niveau hiérarchique.

Modalités d'inscription et de financement

Tarif : Sur demande. Nous contacter via le formulaire de contact à votre disposition en bas de page.

- Possibilité de prise en charge financière par des organismes de financement (OPCO).
- Accès immédiat à la plateforme E-learning après inscription.
- Formation disponible à tout moment, sans contrainte de planning.

Objectifs pédagogiques

- Renforcer la compréhension des menaces courantes en cybersécurité (phishing, ransomware, ingénierie sociale, deepfake...)
- Promouvoir l'adoption de bonnes pratiques sécuritaires au quotidien
- Sensibiliser à l'importance de la sécurité physique et numérique des postes de travail

Contenu de la formation

Chaque module est conçu pour fournir des connaissances pratiques et des compétences applicables, renforçant ainsi la posture de sécurité globale de l'organisation.

- **Phishing**
  - Apprendre à identifier et à éviter les tentatives de hameçonnage par courriel, une méthode courante utilisée par les cybercriminels pour obtenir des informations sensibles.
- **Phishing par téléphone**
  - Découvrir les techniques de hameçonnage vocal, ou « vishing », et les stratégies pour s'en protéger efficacement.
- **Ingénierie sociale**

  - Comprendre les manipulations psychologiques employées pour inciter à divulguer des informations confidentielles et comment y résister.
- **Ransomware**
  - S'informer sur les logiciels de rançon, leur mode de propagation et les mesures préventives pour protéger vos données.
- **Sécurité du cloud**
  - Explorer les meilleures pratiques pour sécuriser les services et les données hébergées dans le cloud, en assurant leur confidentialité et leur intégrité.
- **Réseaux sociaux**
  - Apprendre à utiliser les plateformes sociales de manière sécurisée, en protégeant vos informations personnelles et professionnelles.
- **Sécurité du poste de travail**
  - Découvrir les mesures essentielles pour protéger votre ordinateur contre les menaces internes et externes.
- **Écran vide et bureau propre**
  - Adopter des habitudes visant à protéger les informations sensibles en assurant la confidentialité de votre espace de travail.
- **Navigation internet et réseaux sociaux**
  - Identifier les risques associés à la navigation en ligne et aux interactions sur les réseaux sociaux, et apprendre à les atténuer.
- **Wi-Fi**
  - Comprendre les vulnérabilités des réseaux sans fil et les précautions à prendre pour une connexion sécurisée.
- **Nomadisme et télétravail**
  - Découvrir les bonnes pratiques pour maintenir la sécurité des informations lors du travail à distance ou en déplacement.
- **Accès MFA et mots de passe**
  - Appliquer les bonnes pratiques avec l'authentification multifactorielle et la gestion sécurisée des mots de passe pour protéger vos comptes.
- **Supports amovibles**
  - S'informer sur les risques liés à l'utilisation de dispositifs de stockage externes et les mesures pour les utiliser en toute sécurité.
- **Sécurité physique**
  - Prendre conscience de l'importance de protéger physiquement les équipements et les locaux pour prévenir les accès non autorisés.
- **Deepfake**
  - Découvrir les techniques de falsification numérique et les méthodes pour détecter et se protéger contre ces manipulations.
- **Utilisation de l'IA**
  - Explorer les implications de l'intelligence artificielle en matière de sécurité de l'information et les précautions à prendre lors de son utilisation.

Organisation de la formation

Equipe pédagogique

Notre équipe pédagogique est composée d'experts en sécurité de l'information possédant une vaste expérience dans l'accompagnement d'organisations vers une protection optimale de leurs données sensibles. Leur expertise approfondie leur permet de transmettre les méthodologies et connaissances essentielles pour appliquer directement les meilleures pratiques de sécurité au sein de votre entreprise.

- ❖ Sarah BENBOUZID – Formatrice/Evaluatrice en management de la qualité ISO 9001 et Management des Systèmes d'Information SIO 27001 (Certifications : ISO/IEC 27005 Risk Manager, ISO/IEC 27001 Lead Implementer, ISO/IEC 27001 Lead Auditor, Lead Auditeur CQI and IRCA Qualité ISO 9001)

- Sabri BOUBETRA – Formateur/Evaluateur en management des Systèmes d'Information ISO 27001 et HDS (Master en Cybersécurité, défense des systèmes d'informations, Lead Auditor ISO 27001)
- Médérik GOURDEL - Formateur en management des Systèmes d'Information ISO 27001 (Diplôme : CONCEPTEUR DE SYSTEMES D'INFORMATION)
- Clément JUHEL - Formateur en management des Systèmes d'Information ISO 27001 (Lead Implementer ISO 27001)
- Audrey HELENE - Formatrice en management des Systèmes d'Information ISO 27001 et RGPD/DPO (Diplôme : Master de Droit)
- Dadan KARDIANA - Formateur en management des Systèmes d'Information ISO 27001 (Formation : Adjoint RSSI)
- Khadidja MBOW - Formatrice en management des Systèmes d'Information ISO 27001 (Diplôme : Master Sciences – Technologies : spécialité TDSI)
- Hanane ABDEDOU - Formatrice en management de la qualité ISO 9001/14001 et RSE/HST (Master en management de la qualité, Formations des fondamentaux de l'HST et RSE)
- Francois MAUGER – Formateur RGPD et réglementaire (Certificat d'Aptitude à la Profession d'Avocat)
- Luc MARTIN – Formateur en management des Systèmes d'Information ISO 27001

Moyens pédagogiques et techniques

Notre sensibilisation adopte une approche pédagogique diversifiée pour garantir une compréhension approfondie et une application pratique des concepts. Les méthodes utilisées incluent :

- **Apports théoriques** : présentations structurées des principes fondamentaux de la cybersécurité et des menaces actuelles.
- **Analyses de cas concrets** : études de situations réelles (attaques, incidents) pour faciliter la reconnaissance des menaces dans le contexte professionnel.
- **Fourniture de méthodes et d'exemples** : partage d'outils pratiques, de réflexes et d'exemples pertinents pour adopter les bons comportements sécuritaires au quotidien.

Les outils pédagogiques employés comprennent :

- **16 modules vidéos E-learning au choix** : contenus pédagogiques accessibles à tout moment sur la plateforme, permettant aux apprenants de sélectionner les modules les plus pertinents selon leur profil et leurs risques.
- **Cette combinaison de méthodes** vise à offrir une expérience d'apprentissage engageante, intégrant des scénarios interactifs et des mises en situation réalistes.

Dispositif de suivi de l'exécution d'évaluation des résultats de la formation

Pour assurer le suivi de l'exécution et l'évaluation des résultats de notre sensibilisation, nous mettons en place les dispositifs suivants :

- **Relevé des connexions et taux de complétion** : suivi automatique de l'avancée de chaque collaborateur sur la plateforme E-learning, module par module.
- **Quiz en ligne (E-learning)** : des questionnaires interactifs sont proposés tout au long de la formation pour évaluer la compréhension des concepts abordés et renforcer l'apprentissage.

- **Attestation de suivi** : une attestation est remise à chaque collaborateur ayant complété les modules, permettant de justifier de la formation auprès des organismes de certification (ISO 27001, HDS, SecNumCloud, RGPD).

Ces dispositifs garantissent la traçabilité de la sensibilisation et répondent aux exigences de la norme ISO 27001 (annexe A.7.2.2), du RGPD (article 39) et des cadres sectoriels HDS et SecNumCloud en matière de formation du personnel.

Accessibilité pour tous :

La loi du 5 septembre 2018 pour la « liberté de choisir son avenir professionnel » a pour objectif de faciliter l'accès à l'emploi des personnes en situation de handicap. Notre organisme tente de donner à tous les mêmes chances d'accéder ou de maintenir l'emploi. Nous pouvons adapter certaines de nos modalités de formation, pour cela, nous étudierons ensemble vos besoins. Référent handicap : Stéphanie Paris, sparis@feelagile.com