Deletec

Cybersécurité & Cloud services

Tech IT easy.

Sensibilisation aux risques de cybersécurité

DELETEC propose un programme complet de sensibilisation aux risques de cybersécurité, conçu pour renforcer la vigilance des utilisateurs et réduire les incidents liés aux comportements humains - aujourd'hui responsables de la très grande majorité des compromissions.

↘ Notre approche

La sensibilisation des équipes n'est plus un simple "plus" : c'est un pilier stratégique et une obligation pour toute organisation souhaitant protéger ses activités.

Elle répond également à plusieurs exigences réglementaires et contractuelles essentielles :

- **Les assurances cyber** demandent désormais des preuves régulières de formation pour garantir la couverture des risques.
- **Le RGPD** impose des mesures organisationnelles solides, incluant la formation des collaborateurs à la sécurité des données.
- De plus en plus de clients, partenaires et donneurs d'ordre exigent **des garanties tangibles** en matière de cybersécurité avant d'engager une collaboration.

Avec notre offre de sensibilisation et de simulation de phishing, vos équipes développent les bons réflexes, réduisent immédiatement votre surface de risque et renforcent la conformité exigée par votre écosystème.

Le Volet
Formation à distance

DELETEC conçoit et déploie des programmes de sensibilisation personnalisés visant à transformer le maillon humain - souvent considéré comme le plus vulnérable - en véritable acteur de la cybersécurité.

Le dispositif repose sur une approche complète, alliant communication, pédagogie et évaluation continue :

- **Conception et diffusion de fiches de bonnes pratiques en hygiène informatique** : documents synthétiques et visuels, élaborés selon les recommandations de l'ANSSI, diffusés en ligne ou imprimés. Chaque fiche aborde un thème clé de la sécurité.

- **Sessions de sensibilisation interactives :** ateliers dynamiques, en présentiel ou distanciel, animés par des formateurs certifiés et illustrés d'exemples concrets issus d'incidents réels.

Ces sessions favorisent la mémorisation grâce à des jeux de rôle, quiz et études de cas adaptés au secteur d'activité du client.

Objectifs

- Comprendre les menaces actuelles : phishing, ransomware, ingénierie sociale...
- Identifier les signes d'un e-mail ou d'un site frauduleux
- Adopter les bons comportements numériques au quotidien
- Contribuer à la sécurité globale de l'organisation

Modalités et déroulement de la prestation

Atelier de sensibilisation
(1h, distanciel – groupe de 10 pers. max)

Une session interactive animée par un spécialiste :

- Présentation dynamique des menaces et cas concrets
- Quiz en direct et exemples réels de phishing
- Conseils pratiques adaptés à vos usages professionnels

Le Volet
Campagne de Phishing

Les campagnes de phishing permettent de simuler des attaques personnalisées pour tester la vigilance de vos équipes.

Cette démarche s'inscrit dans un cycle vertueux d'apprentissage, permettant de développer une véritable culture cyber partagée, et de répondre aux exigences de conformité (NIS2, RGPD, ISO 27001).

- **Campagnes de phishing simulées et exercices pratiques** : scénarios de simulation envoyés aux utilisateurs pour mesurer leur réaction et identifier les axes de progression. Les résultats sont anonymisés et consolidés dans un tableau de bord clair et pédagogique.

- **Rapports de synthèse et plan de progrès :** production d'indicateurs de performance (taux de clics, taux de signalement, progression dans le temps) et accompagnement des responsables de la sécurité dans la mise en œuvre d'un plan d'amélioration continue.

Modalités et déroulement de la prestation

Durée de la campagne : 3 à 4 semaines.

- **Conception du message (email de simulation)** : création d'un email crédible, adapté au contexte de l'entreprise.

- **Conception de la fausse page (landing page de sensibilisation)** : création d'une page factice non malveillante, servant uniquement de support pédagogique.

- **Lancement de la campagne par vagues**

- **À la fin de la campagne** : rapport détaillé sur le taux de clics, réactions, progression et recommandations concrètes pour renforcer la posture de sécurité.

Outils et technologies déployés

Solutions de sensibilisation :

Microsoft Defender for Office 365 KnowBe4 Security Awareness Platform

Microsoft Defender for Office 365 Plan 2 (Attack Simulation Training)

↘ Avantages et Bénéfices

- **Réduction significative du risque humain :** grâce à un renforcement des réflexes et à une meilleure reconnaissance des menaces

- **Montée en maturité progressive :** les utilisateurs deviennent progressivement acteurs de leur propre sécurité

- **Conformité réglementaire renforcée :** alignement sur les recommandations ANSSI, NIS2, RGPD, et normes ISO 27001 / 27002

- **Approche sur mesure :** contenus et campagnes personnalisés selon les métiers, les niveaux techniques et les profils utilisateurs

- **Suivi et reporting continus**

- **Soutien à la culture RSE** et numérique responsable

Bénéfices en matière de conformité et de gouvernance :

- **Conformité aux obligations de sensibilisation** prévues par la directive NIS2, le RGPD (article 39) et les normes ISO/IEC 27001 – 27002

- **Production d'éléments de preuve exploitables** lors d'audits internes ou externes (journalisation des sessions, indicateurs de participation, résultats anonymisés)

- **Contribution à la mise en œuvre du plan de sécurité numérique** (PSN) pour les entités publiques et parapubliques

- **Renforcement du dispositif global de gestion des risques**, en conformité avec les bonnes pratiques de gouvernance recommandées par l'ANSSI.

↘ L'atout Deletec

DELETEC se positionne comme un acteur global de la cybersécurité, combinant expertise technique, conseil stratégique et accompagnement humain.

- **Une équipe d'experts certifiés ISO 27001, Microsoft et KnowBe4,** capables de piloter l'ensemble du cycle de sensibilisation, du design à la restitution des résultats ;

- **La conception de parcours de sensibilisation sur mesure,** incluant le branding du client, la contextualisation sectorielle et des scénarios réalistes inspirés d'incidents réels ;

- L'intégration fluide aux environnements Microsoft 365, sans ajout de complexité pour les équipes IT ;

- **La capacité de DELETEC à combiner accompagnement fonctionnel et supervision technique,** garantissant la cohérence du dispositif avec les politiques internes de sécurité et de conformité ;

- **Un reporting exécutif** orienté résultats, permettant d'impliquer les directions générales et de démontrer la valeur concrète des actions de sensibilisation.

Nous contacter

01 53 25 06 60
contact@deletec.fr