IT-SECURITE
Au centre l'Humain

Fiche de présentation

« Campagne de sensibilisation & de formation »

Détails :

Nous réalisons des campagnes de sensibilisation et de formation à la carte selon vos besoins. Ces campagnes de sensibilisation peuvent être des guides, des affiches et des campagnes de communication ou de formation* sur un thème prédéfini ensemble.

* Les formations ne sont pas éligibles CPF et ne sont pas référencées comme tel.

Déroulement :

Vous nous faites part de votre projet, et sous 48h, vous obtiendrez une réponse. Nous nous engageons uniquement sur des projets sur lesquels nous pouvons répondre. Si vous obtenez une réponse négative, c'est que nous n'avons pas la maitrise du sujet.

Exemples de campagne de sensibilisation :

- ✓ **Sensibilisation au phishing :** création d'affiches, d'emails, de guides dédiés au phishing. Les guides permettront à vos collaborateurs de toujours avoir sous la main les étapes clés pour détecter du phishing.

- ✓ **Sensibilisation au mot de passe :** création d'affiche, d'email, de guides dédiés aux mots de passe. Les guides permettront à vos collaborateurs d'avoir des aides mémo-techniques pour avoir un mot de passe sécurisé et personnel et unique pour chaque types d'accès.

- ✓ **Sensibilisation au télétravail et au BYOD :** création d'affiche, d'email, de guides dédiés au télétravail. Les guides permettront à vos collaborateurs de prendre conscience des risques inhérents au télétravail et à l'utilisation des équipements personnels dans un cadre professionnel.

Exemples de formation :

Titre	Public/Niveau	Résumé	Atelier pratique	Durée
Découverte de la sécurité de l'information	Tout collaborateur. Tout niveau.	Permet de découvrir les enjeux, les types d'attaques et les conséquences pour une entreprise et ces collaborateurs.	Non	½ journée
Sécurité et authentification	Tout collaborateur. Tout niveau.	Présentation et explication des éléments clés pour se protéger face à nos outils numériques. Nous abordons les thèmes des accès (mots de passe, authentification multi-facteurs), de la protection des données (classification de l'information, sauvegarde) et de l'utilisation des réseaux (wifi, bluetooth, RFID).	Oui	1 journée
Sécurité et internet	Tout collaborateur. Niveau de connaissance des outils numérique basique.	Présentation et explication des éléments clés pour se protéger sur Internet. Nous abordons les thèmes de la navigation sur Internet, de la messagerie électronique et du téléchargement.	Non	½ journée
Sécurité des postes de travail et des mobiles	Tout collaborateur. Niveau de connaissance des outils numériques basique.	Présentation et explication des éléments clés pour protéger son poste de travail (pro/privé). Nous abordons les thèmes suivants : les applications et leurs mises à jour, les configurations de base en matière de sécurité et la sécurité des périphériques.	Non	½ journée
Sécurité du nomadisme et du BYOD*	Tout collaborateur amené à utiliser son matériel personnel ou itinérant. Niveau de connaissance des outils numériques basique.	Présentation du nomadisme et du BYOD avec présentation des bonnes pratiques à mettre en place pour se prémunir de toutes menaces. Séparation des usages pro/privée. **BOYD : Bring Your Own Device (EN), apporter vos équipements personnels (FR).*	Oui	½ journée
Sécurité et Ingénierie sociale	Tout collaborateur ayant un poste stratégique dans l'entreprise. Tout niveau.	Présentation et explication du « social engineering ». Apprendre les bonnes pratiques pour s'en prémunir. Apprendre à séparer vie privée et vie professionnelle sur les réseaux sociaux.	Oui	½ journée

Protéger ses actifs, son entreprise et ses collaborateurs grâce à la charte informatique.	Responsable informatique ou sécurité.	Nous verrons, comment et pourquoi mettre en place une charte informatique. Et ce qu'elle peut et doit contenir pour protéger toutes les parties prenantes au sein de l'entreprise.	Oui	1 journée
Continuité des affaires grâce au PRA.	Responsable informatique ou sécurité.	Présentation et explication des bénéfices que peuvent apporter la mise en place d'un Plan de Reprise d'Activité (PRA) au niveau de l'IT.	Oui	1 journée
Sécurité, phishing et ransomware	Tout collaborateur. Tout niveau.	Présentation et explication des menaces que représentent le phishing et le ransomware pour l'entreprise et ses collaborateurs.	Oui	½ journée

Pour information, ces exemples ne sont pas exhaustifs, nous pouvons personnaliser ces formations selon vos besoins mais également combiner plusieurs thèmes.

La durée présentée est indicative pour 12 personnes maximum par session. Des ateliers pratiques sont disponibles pour certaines formations, ils permettent de mettre en pratique, avec un accompagnement, des mesures présentées.