Programme de formation à l'hygiène numérique

Version à jour du 15/05/2024

Résumé :

Cette formation vise à former tout personnel de tout secteur d'activité à l'hygiène numérique et aux bons gestes à effectuer en cas d'attaques informatiques.

Prérequis : Aucun

Localisation : France + pays francophone en présentiel (les formateurs se déplacent dans vos locaux).

Public visé : Tous publics

Contact : contact@sentionis.fr

Grille tarifaire :

Nombre de personnes à former	Prix par personnes
Supérieur à 50	100€
À partir de 50	95€

La décomposition en groupe et le nombre d'interventions seront discutés avec le collaborateur afin d'assurer le meilleur suivi possible.

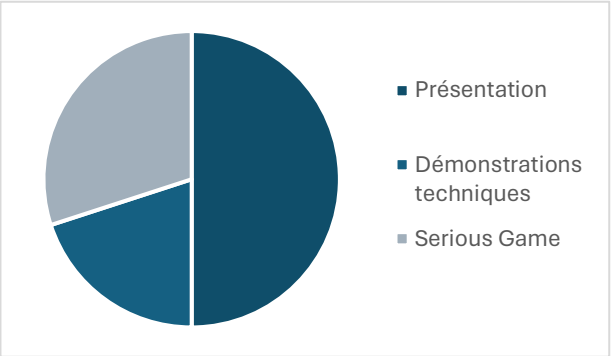
Recommandation de formation : Tout collaborateur ayant accès au SI et en priorité tout individu dans/ou proche du CoEx/CoDir, puis tous les 2 ans.

Durée : 3 heures – 4 heures.

Personnalisation : Oui – La formation n'est pas standardisée, les formateurs interviennent en présentiel et savent adapter leur discours aux différents profils et présentation aux cas concrets de votre société. Une réunion sera prévue en amont avec vous afin d'être au plus proche des besoins et attendus.

Méthodes :

- Présentation (avec temps d'échanges)
- Démonstrations techniques
- Serious Game



Attestation : Oui – Fournie en fin de formation.

Compétences développées :

- Connaître les types d'attaques les plus courantes ;
- Utiliser l'outil numérique avec les meilleures pratiques en termes de cybersécurité ;
- Adopter les bons gestes face à une attaques.

Programme :

- **Mots de passe :**
  - Création & robustesse d'un mot de passe ;
  - Comment les stocker ?
  - Fuite de données.
- **Phishing :**
  - Le phishing, c'est quoi ?
  - Les indices pour identifier le phishing ?
  - Les autres types de phishing (spear-phishing…).
- **RPGD & Obligations légales :**
  - RGPD c'est quoi et que permet-il ?
  - Obligations juridiques de l'employeur.
  - Obligations juridiques de l'employé.
- **Les supports USB**
  - Anodin une clé USB ?
  - Gestes à adopter ?
- **Ransomware**
  - Qu'est-ce que c'est ?
  - Comment infectent-ils le poste/le réseau de l'entreprise ?
  - Les conséquences ?
- **Sécurité de terminaux mobiles ?**
  - Accès physique ;
  - Mises à jour ;
  - Applications, les indices d'un comportement malveillant ;
  - Wifi ouvert : ami ou ennemi ?
- **Ingénierie sociale**
  - Qu'est-ce que c'est ?
  - Les techniques ?
- **Sauvegarde de données**
  - Local, Cloud, hors ligne… ?
  - Sauvegarder c'est bien, savoir restaurer c'est mieux.

Les différents modules seront accompagnés de démonstrations techniques.

Démonstrations techniques :

- Phishing
- Clé USB
- Ransomware

Formateurs : Nos formateurs ont chacun plusieurs années d'expérience en cybersécurité au sein de grands groupes. Ils interviennent en présentiel avec pédagogie auprès de vos équipes.