Se sensibiliser à la cybersécurité : acquérir les bonnes pratiques

1 jour(s) - 3,50 heure(s)

Programme de formation

Public visé

tous les collaborateurs utilisateurs d'un ordinateur

Pré-requis

Aucune connaissance particulière
Maitriser son matériel informatique personnel ou professionnel

Objectifs pédagogiques

Comprendre les techniques des pirates informatiques
Appréhender les attaques

Description / Contenu

Se familiariser avec le jargon de la cybersécurité

- Lister les programmes informatiques malveillant
    - backdoor, botnet, brute force, bug bounty, chiffrement

- Comprendre leur principe et fonctionnement

Se protéger des menaces
Connaître les différents types d'attaques informatiques
- Comprendre le principe des attaques de masse
    - Le Botnet

- Comprendre le principe des attaques ciblées sous ses différentes variantes
  - Hameçonnage
  - Le piratage de compte en ligne
  - L'arnaque au faux support technique
  - Cyberharcèlement
  - Violation de données personnelles
  - Rançongiciels ou ransomwares
  - Spams
  - Faux ordres de virement
  - Virus
  - Comprendre les motivations des hackers
  - Sensibiliser les collaborateurs
  - Se protéger des attaques

Concevoir un mot de passe fort
- Identifier un mot de passe fort
- Savoir créer un mot de passe fort
- Connaître la technique de la phrase sous forme de mot de passe

Gérer ses mots de passe
- Apprendre à gérer ses mots de passe
- Connaître les différentes solutions de gestion

Reconnaitre le principe de l'hameçonnage (le phishing)
- Connaître le principe du phishing
- Se familiariser avec les différentes techniques employées par les hackers
- Donner quelques exemples d'attaques
  - Développer les 5 méthodes courantes de l'ingénierie sociale
  - Comprendre leur fonctionnement

Détecter et éviter les ransomware
- Connaître le ransomware
- Reconnaître les techniques utilisées par les pirates informatiques
- Donner les bonnes pratiques en cas d'attaque

Être prudent avec les appareils de connexion
- Apprendre à cloisonner le professionnel et le personnel
- Créer des sessions différentes pour chaque usage et utilisateur
- Se méfier des objets connectés

Naviguer sur le net
- Identifier un site fiable
  - Rechercher le vendeur sur un moteur de recherche

- Détecter les sites douteux (promotions trop alléchantes)
- Analyser le nom de domaine du site avec un outil
- Surveiller la présence du protocole sécurisé HTTPS
- Vérifier les Conditions Générales de Vente et les mentions légales

Les paiements sécurisés
- Choisir la double sécurité avec votre banque
- Vérifiez que la page est bien sécurisée
- Prenez garde aux sites inconnus et aux offres trop alléchantes
- Évitez d'enregistrer vos coordonnées bancaires
- Se méfier des réseaux WiFi publics
- Assurez votre sécurité numérique globale

Le système
- Sauvegarder vos données sur une source externe
- Vérifier vos mises à jour

Modalités pédagogiques

Formation animée en présentiel ou classe virtuelle

Action par groupe de 1 à 8 personnes maximum

Horaires : 09h00-12h30 / 13h30-17h00

Moyens et supports pédagogiques

Alternance entre théorie et pratique.

Modalités d'évaluation et de suivi

Qu'il s'agisse de classe virtuelle ou présentielle, des évaluations jalonneront la formation : tests réguliers des connaissances, cas pratiques, ou validation par une certification à l'issue de l'action par les stagiaires, au regard des objectifs visés

Accessibilité

Nos formations sont accessibles aux personnes en situation de handicap.

Afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous.
Un entretien avec notre référent handicap pourra être programmé afin d'identifier les besoins et aménagement nécessaires.

Délai d'accès

- Pour les formations intra : Les modalités et délais d'accès sont à valider lors d'un entretien téléphonique préalable et selon disponibilités respectives.

- Pour les formations inter : Selon notre calendrier d'inter-entreprises