

Cybersécurité, prévenir les risques et adopter les bons réflexes

Dans un contexte où les usages numériques occupent une place croissante dans l'activité quotidienne de l'entreprise, les collaborateurs sont régulièrement exposés à différents risques liés à la cybersécurité : phishing, usurpation d'identité, fraude, compromission de comptes, perte de données ou utilisation inadaptée d'outils numériques.

L'entreprise souhaite ainsi sensibiliser ses salariés aux principales menaces cyber et renforcer les bonnes pratiques à adopter dans leurs usages professionnels, que ce soit sur la messagerie, les mots de passe, les équipements, le télétravail, les outils de partage ou encore l'intelligence artificielle.

La formation vise à développer une culture commune de la cybersécurité, à réduire les comportements à risque et à permettre aux participants d'identifier plus rapidement une situation suspecte afin d'adopter les bons réflexes et de réagir efficacement en cas d'incident.

Formation en présentiel ou à distance, en inter-entreprise ou en intra-entreprise

Informations pratiques

- **Public** : Toute personne utilisant des outils numériques dans le cadre de son activité professionnelle
- **Prérequis** : aucun
- **Durée** : 1 jour (07h)
- **Personnes en situation de handicap** : notre page dédiée vous donnera toutes les informations concernant l'accessibilité de nos formations aux personnes en situation de handicap
<https://www.formavictoire.com/handicap>
- **Tarif formation intra-entreprise** : 1 490€ HT par jour (groupes de 2 à 10 personnes)
- **Tarif formation inter-entreprise** : 390 € HT par jour et par apprenant
- **Tarif accompagnement individuel** : 150 € HT par heure
- **Délai d'accès** : 3 semaines entre la demande et l'animation de la formation (réunion de préparation, choix du formateur, planification de la session, information des participants)

Evaluations

- **Modalité d'adaptation** : Le contenu des modules de formation peut être adaptés aux besoins spécifiques des stagiaires.
- **Suivi de l'assiduité** : Feuilles de présence signées par demi-journée, ou rapport de connexion et signature d'une feuille d'émargement en distanciel.
- **Evaluation début de formation** : Questionnaire de positionnement
- **Evaluations en cours de formation** : QCM, exercices, quiz, compte rendu pédagogique en fin de chaque session
- **Evaluations en fin de formation** : Evaluation des acquis
- **Evaluation de la satisfaction** : Compte rendu pédagogique du formateur, évaluation de satisfaction du client, évaluation de satisfaction des apprenants en fin de formation.
- **Evaluations après la formation** : Evaluation à froid des apprenants 4 à 6 mois après la formation (Transfert des compétences)
- **Attestation de fin de formation** : Cybersécurité : prévenir les risques et adopter les bons réflexes

Extensions Possibles

- Organiser des ateliers thématiques post-formation pour approfondir des sujets spécifiques comme le phishing, les mots de passe, la protection des données ou les usages de l'intelligence artificielle.
- Mettre en place des campagnes régulières de sensibilisation afin d'entretenir la vigilance des collaborateurs face aux nouvelles menaces cyber.
- Proposer des simulations de phishing pour permettre aux salariés de tester leurs réflexes dans des situations proches de la réalité.
- Organiser des exercices collectifs de simulation d'incident afin de renforcer les réflexes de signalement et la capacité à réagir rapidement face à une situation suspecte.

Méthodes pédagogiques

- 80% pratique et 20% théorique
- Mises en situation
- Études de cas
- Jeux de rôles, pratiques interactives.
- Débriefings
- Apports théoriques en lien avec la pratique
- Tutoriels en ligne

Objectifs

Objectif global de la formation :

- Être capable d'identifier les principaux risques liés à la cybersécurité, d'adopter les bonnes pratiques de prévention et de réagir efficacement face à une situation ou un incident suspect.

Objectifs de chaque module :

- Identifier les cybermenaces et leurs impacts sur l'entreprise
- Détecter les tentatives de phishing et d'ingénierie sociale
- Renforcer la sécurité de ses mots de passe et de ses compte
- Sécuriser son poste de travail et ses équipements mobiles
- Sécuriser le télétravail, la mobilité et les connexions Wi-Fi
- Protéger les données et informations de l'entreprise
- Prévenir les risques cyber liés à l'intelligence artificielle
- Réagir efficacement face à un incident de cybersécurité

PROGRAMME

MODULE 1 – IDENTIFIER LES CYBERMENACES ET LEURS IMPACTS SUR L'ENTREPRISE

- Définir la cybersécurité et comprendre ses enjeux dans le contexte professionnel.
- Identifier pourquoi toutes les entreprises peuvent être exposées aux cybermenaces.
- Reconnaître les principales menaces :
 - Phishing,
 - Ransomware
 - Logiciels malveillants
 - Vol d'identifiants,
 - Usurpation d'identité
 - Fraude au président
 - Fraude au changement de RIB
- Identifier les conséquences possibles d'une cyberattaque sur l'activité
 - L'interruption d'activité
 - Les données
 - Les finances
 - L'image de l'entreprise
 - Les clients et partenaires.
- Comprendre le rôle de chaque salarié dans la prévention des risques et la sécurité globale de l'entreprise.
- **Mise en situation** : Analyser plusieurs scénarios professionnels afin d'identifier les cybermenaces et les bons réflexes à adopter.

MODULE 2 – DÉTECTER LES TENTATIVES DE PHISHING ET D'INGÉNIERIE SOCIALE

- Comprendre le fonctionnement d'une attaque de phishing.
- Identifier les signes permettant de reconnaître un e-mail suspect.
- Vérifier l'adresse réelle de l'expéditeur.
- Repérer les faux liens et les pièces jointes frauduleuses.
- Reconnaître les techniques de manipulation basées sur l'urgence.
- Identifier les fraudes par SMS, QR code et appel téléphonique.
- Repérer les usurpations de dirigeants, fournisseurs ou services informatiques.
- Adopter les bons réflexes avant de cliquer.
- Savoir réagir après avoir cliqué par erreur.
- **Mise en situation** : Analyser plusieurs e-mails afin d'identifier les tentatives de phishing.

MODULE 3 – RENFORCER LA SÉCURITÉ DE SES MOTS DE PASSE ET DE SES COMPTE

- Identifier les erreurs les plus fréquentes dans la gestion des mots de passe.
- Construire un mot de passe robuste et sécurisé.
- Comprendre les risques liés à la réutilisation d'un même mot de passe.
- Utiliser un gestionnaire de mots de passe pour sécuriser ses accès.
- Comprendre le fonctionnement et l'intérêt de l'authentification multifacteur (MFA).
- Adopter les bons réflexes lorsqu'un mot de passe est compromis.
- Sécuriser efficacement ses comptes professionnels.
- **Mise en situation** : Identifier les bonnes et mauvaises pratiques d'authentification.