CONNECT E-FORM

Boostez vos compétences avec l'innovation digitale

« CYBERSÉCURITÉ POUR LES COLLABORATEURS »

PRÉSENTATION DE LA FORMATION POUR LES PROFESSIONNELS

Réf. : FND54A

ADOPTER LES BONS RÉFLEXES EN CYBERSÉCURITÉ ET RÉDUIRE LES RISQUES HUMAINS

Comprendre la cybersécurité, c'est déjà protéger l'entreprise et ses données.

Grâce à une approche claire, progressive et non technique, vous découvrirez les principales menaces numériques, les comportements à risque et les bonnes pratiques à adopter au quotidien. L'objectif est de réduire les incidents liés au facteur humain et de renforcer durablement la sécurité de l'organisation.

CE QUE VOUS ALLEZ APPRENDRE

- **Comprendre Comprendre les enjeux de la cybersécurité en entreprise,**
- **Identifier les principales cybermenaces actuelles,**
- **Reconnaître les tentatives de phishing et de fraude,**
- **Sécuriser son poste de travail et ses accès,**
- **Adopter une hygiène numérique responsable,**
- **Appliquer les bonnes pratiques RGPD au quotidien,**
- **Savoir réagir efficacement en cas d'incident,**
- **Ancrer des réflexes de sécurité durables.**

En suivant cette formation, vous bénéficierez de :

- **Contenus structurés et accessibles à tous,** sans prérequis technique,
- **Cas concrets** inspirés de situations réelles,
- **Outils pratiques et de check-lists** immédiatement utilisables.

Que vous soyez collaborateur, manager ou fonction support, **adoptez les bons réflexes pour contribuer activement à la sécurité numérique de votre entreprise.**

OBJECTIFS GLOBAUX PÉDAGOGIQUES

A l'issu de la formation, les apprenants seront capables de :

- Expliquer les enjeux et risques liés à la cybersécurité,
- Identifier les tentatives de fraude et de phishing,
- Appliquer les bonnes pratiques de sécurité numérique,
- Sécuriser leur poste de travail et leurs accès,
- Respecter les principes essentiels du RGPD,
- Réagir de manière appropriée face à un incident,
- Adopter un comportement responsable et préventif.

THÉMATIQUES

- **Comprendre les enjeux de la cybersécurité en entreprise,**
- **Reconnaître le phishing et les tentatives de fraude,**
- **Sécuriser son poste de travail et ses accès,**
- **Bonnes pratiques numériques & comportements à risque,**
- **RGPD & protection des données au quotidien,**
- **Réagir face à un incident & ancrer les bonnes pratiques.**

CONNECT E-FORM

Boostez vos compétences avec l'innovation digitale

« CYBERSÉCURITÉ POUR LES COLLABORATEURS »

PROGRAMME DE LA FORMATION

Réf. : FND54A

FORMATION INNOVANTE 100% E-LEARNING, QUI ALLIE INTELLIGENCE ET INTERACTIVITÉ

Durée : 7 heures (100 % e-learning)

Objectif : acquérir une maîtrise opérationnelle des bons réflexes en cybersécurité afin de réduire les risques humains, protéger les données et renforcer la sécurité de l'entreprise.

Programme : 6 modules

Vous souhaitez réduire les risques cyber liés aux comportements humains ?

Notre formation **« Cybersécurité pour les collaborateurs »** est conçue pour tous les publics non techniques.

Grâce à une pédagogie simple et des mises en situation concrètes, vous apprendrez à reconnaître les menaces, à sécuriser vos usages numériques et à réagir efficacement face aux incidents, en cohérence avec les règles internes et le RGPD. La cybersécurité devient alors une responsabilité partagée, portée par chaque collaborateur.

LE PROGRAMME EN DÉTAIL

MODULE 1 - COMPRENDRE LES ENJEUX DE LA CYBERSÉCURITÉ EN ENTREPRISE

- Qu'est-ce que la cybersécurité ?
- Panorama des cybermenaces actuelles,
- Le facteur humain : premier risque cyber,
- Conséquences d'une cyberattaque,
- Responsabilité individuelle et collective.

> QCM d'évaluation

MODULE 2 - RECONNAÎTRE LE PHISHING ET LES TENTATIVES DE FRAUDE

- Qu'est-ce que le phishing ?
- Typologies d'attaques,
- Signaux d'alerte,
- Exemples concrets d'attaques réelles.

> QCM d'évaluation

MODULE 3 - SÉCURISER SON POSTE DE TRAVAIL ET SES ACCÈS

- Mots de passe sécurisés & gestionnaires,
- Authentification à double facteur (2FA),
- Verrouillage de session,
- Mises à jour et correctifs,
- Utilisation sécurisée du Wi-Fi,
- Bonnes pratiques en télétravail.

> QCM d'évaluation

MODULE 4 - BONNES PRATIQUES NUMÉRIQUES & COMPORTEMENTS À RISQUE

- Téléchargements & logiciels non autorisés,
- Clés USB & périphériques externes,
- Partage de fichiers et cloud,
- Réseaux sociaux & ingénierie sociale,
- Séparation usages pro / perso,
- Réflexes à adopter en cas de doute.

> QCM d'évaluation

MODULE 5 - RGPD & PROTECTION DES DONNÉES AU QUOTIDIEN

- Qu'est-ce qu'une donnée personnelle ?
- Principes fondamentaux du RGPD,
- Données sensibles,
- Bonnes pratiques de collecte, stockage et partage,
- Confidentialité & droit d'accès,
- Erreurs fréquentes des collaborateurs.

> QCM d'évaluation

MODULE 6 - RÉAGIR FACE À UN INCIDENT & ANCRER LES BONNES PRATIQUES

- Que faire ?
- Qui alerter et comment ?
- Règles internes & procédures,
- Bonnes pratiques durables,
- Responsabilisation des collaborateurs,
- Plan d'actions individuel.

> QCM d'évaluation

COMMENCEZ DÈS AUJOURD'HUI !
La cybersécurité ne repose pas uniquement sur la technique...

... Faites de chaque collaborateur un **acteur vigilant, responsable et engagé dans la protection des données et de l'entreprise.**

CADEAU DE BIENVENUE !

Documents BONUS à télécharger

OFFERTS
POUR TOUTE INSCRIPTION

CONNECT E-FORM
Boostez vos compétences avec l'innovation digitale

SCANNEZ-MOI !

RÉSERVEZ DÈS MAINTENANT VOTRE 1ER RENDEZ-VOUS SUR CALENDLY

06 70 74 67 80 contact@connect-e-form.fr www.connect-e-form.fr

CONNECT E-FORM 16 Rue Saint-Antoine du T, Bureau 3 31000 Toulouse - France
SARL au capital de 100 € - Code APE : 721Z - N° TVA : FR16988093670 - RCS Toulouse