Sensibilisation aux risques informatiques pour collaborateurs

CYBERSÉCURITÉ

Objectifs	Former les collaborateurs aux risques numériques les plus courants - Détecter les tentatives de fraude (phishing, rançongiciels...) - Protéger leur poste de travail - Adopter de bons réflexes en télétravail - Mieux comprendre leur rôle dans la protection des données de l'entreprise.
Participants	Collaborateurs administratifs - Commerciaux - Comptables - Responsables RH - Assistants de direction - Managers d'équipe - Agents de service client - Employés en télétravail
Prérequis	Notions basiques en cybersécurité - bonnes pratiques numériques - reconnaissance du phishing et ingénierie sociale - sensibilisation au mot de passe - usage sécurisé des outils collaboratifs.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation
Méthodes pédagogiques	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	400 € HT
Durée	0.5 jours - 4 heure(s)
Modalités et délais d'accès	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

Code : NCI_KM5EHWUH

Mis à jour le : 25 mars 2026

Programme :

Introduction
Présentation de la formation
Pourquoi la cybersécurité est l'affaire de tous
Quelques chiffres clés sur les cyberattaques
Lexique simple de la cybersécurité

Comprendre les menaces
Virus, vers, rançongiciels, logiciels espions
Phishing : détecter un faux mail
Arnaques par téléphone ou SMS
Failles de sécurité et erreurs humaines
Applis ou logiciels suspects

Utilisation sécurisée de l'ordinateur
Bonnes pratiques sur Internet
Créer et gérer ses mots de passe
Double authentification
Importance des mises à jour
Sauvegarde des fichiers
Attention aux clés USB, pièces jointes, disques externes
Gérer un comportement suspect de son PC

Télétravail et mobilité
Risques du Wi-Fi public
Sécuriser son smartphone et sa tablette
Se connecter à distance en toute sécurité
Stockage et accès aux fichiers professionnels
Les erreurs fréquentes à éviter en télétravail

Contribuer à la sécurité de l'entreprise
Utiliser le réseau de l'entreprise
Séparer usage pro/perso
Outils de sécurité internes : comprendre leur rôle
La surveillance informatique, pourquoi et comment
Accès à distance : vigilance et sécurité

Règles et responsabilités
Le RGPD expliqué simplement
Ce qu'il est permis ou interdit de faire avec les données
Règles internes de cybersécurité
Réagir rapidement en cas de problème
Qui contacter ? Que faire si on se fait piéger ?

Cas concrets & exercices
Étude de cas : phishing ayant causé une fuite
Quiz interactif : les bons réflexes
Erreurs courantes à éviter
Mise en situation : reconnaître un mail frauduleux
Conseils personnalisés par métier (RH, compta, managers...)

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20

Clôture

- Ce qu'il faut retenir
- Bonnes habitudes à conserver
- Ressources simples pour continuer à se former
- Contact utile en cas de doute

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20