

ACQUÉRIR LES BONS RÉFLEXES POUR SE PRÉMUNIR DES RISQUES CYBER ET PROTÉGER SON ACTIVITÉ EN SITUATION DE TRAVAIL À DISTANCE GÉNÉRALISÉ

### Cybersécurité Plus que jamais ?

Souvent mis en place dans l'urgence pour permettre la continuité de l'activité, le télétravail généralisé peut constituer une faille majeure, quelle que soit la robustesse des pare-feu existants. Tout participe actuellement aux risques d'intrusion, de détournement ou de fraude. En témoigne la recrudescence des attaques.

### Cybersécurité Des comportements avant tout ?

Vos salariés sont en télétravail ? Rempart ou cheval de Troie, le bon réflexe d'un seul de vos collaborateurs peut faire la différence, quand on sait que 4 attaques sur 5 sont introduites par les utilisateurs eux-mêmes. Ne mettez pas la sauvegarde de votre activité en danger à un moment déjà critique pour sa pérennité.

### Cybersécurité Formation ou sensibilisation ?

Plus qu'une sensibilisation aux bons réflexes, la formation par Ancrage Mémoirel® de Woonoz est une formation personnalisée qui permet de réduire significativement l'exposition de votre entreprise au risque cyber.

### Cybersécurité À quoi s'expose-t-on ?

- 42 % des entreprises ont déjà subi une ou plusieurs attaques ou tentatives d'attaque informatique.
- Un tiers des entreprises changent leurs mots de passe peu régulièrement, soit tous les 6 à 12 mois.
- 17 % des entreprises seulement sont assurées contre les attaques informatiques.

Ce parcours en ligne personnalisé est un complément efficace aux ressources mises à disposition sur le portail [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr) et le contenu de la formation est bien sûr conforme aux recommandations publiques.

## Solution

La solution : prescrire à l'ensemble de vos collaborateurs la formation ultra-personnalisée de Woonoz. Quel que soit leur niveau initial, ce parcours en ligne garantit les réflexes de cybersécurité pour une mise en pratique réelle et systématique, au-delà d'une simple sensibilisation.

## Cybersécurité

Capitalisant sur une formation déployée avec succès chez Bureau Veritas, Groupama ou encore Webhelp Payment Services, Woonoz a confié à Inquest l'actualisation du contenu au contexte de confinement pour un parcours parfaitement adapté aux besoins des équipes et des employeurs.

## Preuve

Les techniques de neuro-learning et d'adaptive learning au cœur des formations Woonoz ont apporté la preuve de leur efficacité dans les domaines de la sécurité et de la conformité. Woonoz est aussi à l'origine du Projet Voltaire®, fort de ses 5 millions d'utilisateurs pour la remise à niveau en orthographe.

# Programme

30 à 50  
minutes  
seulement  
pour maîtriser  
29 points clés

## Chapitre 1

Être vigilant quant aux  
cyberattaques

- Se méfier des demandes de mot de passe ou d'identifiant
- Ne pas céder au « chantage »
- Se méfier des demandes jouant sur l'autorité
- Se méfier des liens hypertextes
- Se méfier des pièces jointes
- Se méfier des sites contrefaits
- Se méfier d'un ralentissement ou blocage de l'ordinateur
- Se méfier des demandes de transfert de fonds

## Chapitre 2

Les règles au niveau de l'entreprise

- Cible des attaques
- Tous acteurs de la sécurité informatique
- Appliquer TOUTES les règles, TOUT le temps
- Agir en cas de doute
- Ne pas divulguer d'informations sensibles sur l'entreprise

## Chapitre 3

Sécuriser l'accès à mes services et applications

- Complexifier ses mots de passe
- Complexifier son code PIN
- Mémoriser ses mots de passe
- Protéger les fichiers sensibles par mot de passe

## Chapitre 4

Sécuriser l'accès à mon poste de travail

- Surveiller sa session
- Éteindre son ordinateur
- Installer de nouveaux logiciels
- Activer l'antivirus
- Activer le VPN
- Appliquer les mises à jour sécurité

## Chapitre 5

Télétravailler et collaborer en toute cybersécurité

- Séparer e-mails perso et pro
- Consulter Internet
- Sauvegarder les données
- Transférer des fichiers
- Utiliser sa webcam
- Authentifier un interlocuteur

Pour déployer cette formation dans votre entreprise, association, collectivité ou établissement de service public, rendez-vous sur

[www.woonoz.com/solidarite-cybersecurite/](http://www.woonoz.com/solidarite-cybersecurite/)

WOONOZ en partenariat avec INQUEST

INQUEST est une filiale du groupe Stellant spécialisée en conseil et management des risques de l'IT et du Cyber mais également de la finance, de l'industrie, de l'automobile et de l'aéronautique. Cartographie des risques internes et externes d'entreprise, gestion de crise cyber, incendie ou environnementale, investigations et retours d'expérience, INQUEST agit au cœur des enjeux des entreprises.



contact@woonoz.com • 04 69 64 70 50  
[www.woonoz.com](http://www.woonoz.com)



0 825 87 69 08 • contact@inquest-risk.com  
[www.inquest-risk.com](http://www.inquest-risk.com)