

Formation **Etre capable de protéger ses outils numériques**

PUBLIC	Tous collaborateurs devant acquérir les bonnes pratiques en matière de cybersécurité.
PRE-REQUIS	Aucune connaissance particulière n'est attendue. Il est toutefois recommandé de maîtriser son matériel informatique professionnel.
DUREE	3h30
NB DE PARTICIPANTS	En moyenne 5 et maximum 10
CONDITION D'ACCESSIBILITE	Locaux accessibles aux personnes en situation de handicap
TARIF	Sur devis
DELAI D'ACCES	Sur demande
OBJECTIFS	Mettre en œuvre des solutions pour protéger ses données et son poste de travail. Se poser les bonnes questions pour avoir les bons réflexes dans le cadre de son travail. Identifier les différentes menaces informatiques afin de les éviter. Adopter les règles de sécurité en cas de nomadisme.

CONTENUS	Introduction à la cybersécurité Partie 1 : Protection des données et de son poste de travail - Comment éviter les menaces cyber - Concevoir et gérer des mots de passes fort Partie 2 : Identification des différentes techniques frauduleuses pour obtenir des données - Les différentes techniques de fishing - Comment s'en protéger - Eviter le ransomware Partie 3 : Les règles de sécurité en cas de nomadisme - Définition - Quels sont les risques - Comment se protéger
METHODES MOBILISEES	De nombreux exemples sont introduits dans chaque partie Questionnement, interactivité, Exercices Support diffusé : Powerpoint Supports remis : PowerPoint et Fiche bonnes pratiques en matière de Cybersécurité de cybermalveillance.gouv.fr
MODALITES D'EVALUATION	Questionnaire en fin de formation
INTERVENANT	SAS AESTRIA : I. KOSEM