Aestria
Un monde plus digital, ensemble.

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	½ journée
NB DE PARTICIPANTS	En moyenne 5 et maximum 15
CONDITION D'ACCESSIBILITE	Locaux accessibles aux personnes en situation de handicap
TARIF	Sur devis
DELAI D'ACCES	Sur demande
OBJECTIFS	Renforcer la résilience de l'organisation face aux cybermenaces. Favoriser un changement de mentalité et de comportement des employés vis-à-vis de la sécurité de l'information. Susciter l'adhésion et l'engagement envers les initiatives en matière de cybersécurité. Réduire les erreurs humaines et atténuer les risques de sécurité. Améliorer les résultats des audits et démontrer la conformité aux réglementations.

CONTENUS	Partie 1 : Se protéger des menaces informatiques - Introduction à la cybernétique - Assimilation de certains termes Partie 2 : Concevoir des mots de passe forts - Les critères pour un bon mot de de passe Partie 3 : Gérer ses mots de passe - Introduction aux outils fiable de gestion de mots de passe Partie 4 : Reconnaitre le phishing (hameçonnage) - Introduction aux différents risques - Les bonnes pratiques à adopter Partie 5 : Eviter le rançongiciel - Introduction aux différents risques - Les bonnes pratiques à adopter Partie 6 : Être prudent avec le nomadisme - Les risques du nomadisme - Les bonnes pratiques à adopter De nombreux exemples sont introduits dans chaque partie
METHODES MOBILISEES	Questionnement, interactivité, Exercices Support diffusé : Powerpoint Supports remis : Bonnes pratiques en matière de Cybersécurité
MODALITES D'EVALUATION	Questionnaire en fin de formation et à J+1 mois
INTERVENANT	SAS AESTRIA : I. KOSEM