

**Durée :** 2 jours (14 heures)

**Objectifs :** Sensibiliser les utilisateurs de l'outil informatique à la sécurité :

- ✓ Comprendre les concepts clés liés à l'importance d'assurer la sécurité des informations et des données, d'assurer leur sécurité physique, d'éviter le vol de données personnelles et de protéger la vie privée des utilisateurs.
- ✓ Être capable de protéger un ordinateur, un dispositif numérique mobile, un réseau contre les logiciels malveillants et les accès non autorisés
- ✓ Connaître les différents types de réseaux, de connexions et les composants spécifiques tels que le pare-feu qui peuvent poser des problèmes lors des connexions
- ✓ Naviguer sur le World Wide Web et communiquer en toute sécurité sur internet
- ✓ Comprendre les problèmes de sécurité liés à la communication, notamment en matière de courriers électroniques et de messagerie instantanée
- ✓ Sauvegarder et restaurer des données de manière appropriée et sécurisée, entreposer ses données et ses dispositifs numériques mobiles en toute sécurité

**Public :** Toute personne désirant connaître les concepts essentiels et les techniques à maîtriser pour utiliser de façon sécurisée les TIC en entreprise.

**Pré requis :** Avoir suivi la formation Windows Gestion des documents ou niveau équivalent (Utiliser de façon autonome les fonctionnalités de base de Windows.) ainsi que de savoir utiliser une messagerie et internet

**Test et entretien individuels** pour établir clairement les besoins du stagiaire.

**Programme\* :**

<p><b>Les concepts de sécurité</b></p> <ul style="list-style-type: none"> <li>• Les différentes menaces sur les données</li> <li>• La notion de valeur de l'information</li> <li>• La notion de sécurité personnelle</li> <li>• La notion de sécurité des fichiers</li> </ul> <p><b>Les logiciels malveillants</b></p> <ul style="list-style-type: none"> <li>• Définition et fonctionnement</li> <li>• Les différents types de logiciels malveillants</li> <li>• Comment se protéger des logiciels malveillants</li> </ul> <p><b>La sécurité réseau</b></p> <ul style="list-style-type: none"> <li>• Connaître les principaux types de réseaux</li> <li>• Les différents types de connexions réseau</li> <li>• La sécurité en environnement sans fil (Wi-Fi)</li> <li>• Les différentes possibilités de contrôle d'accès</li> </ul>	<p><b>Utiliser le Web de manière sécurisée</b></p> <ul style="list-style-type: none"> <li>• Sécuriser la navigation Web</li> <li>• Sécuriser son utilisation des réseaux sociaux</li> </ul> <p><b>Pourquoi sécuriser ses communications</b></p> <ul style="list-style-type: none"> <li>• Communiquer de manière sécurisée par courriel</li> <li>• Communiquer de manière sécurisée par messagerie instantanée</li> </ul> <p><b>Gestion de la sécurité des données</b></p> <ul style="list-style-type: none"> <li>• Sécuriser et sauvegarder les données</li> <li>• Détruire les données de manière sécurisée</li> </ul>
--	---

\*Parcours modulables et individualisés. Des programmes détaillés de chaque module sont disponibles sur simple demande.

**Pédagogie :** Enseignement théorique puis manipulation sur ordinateur - l'accent est mis sur la pratique. Mise en situation : cas pratiques sélectionnés en fonction des besoins des stagiaires, définis préalablement.

**Intervenant :** Formateur en informatique.

**Validation :** Remise d'une attestation de formation. Possibilité de passation du module « Sécurité des T.I » du PCIE, selon niveau de départ.