

CLAUDE FONDATIONS · FICHE DE RÉVISION

Sécurité et gestion des informations

Module 17

L'essentiel à retenir

01. Maîtriser les risques liés à l'usage de Claude

Utiliser Claude efficacement, c'est aussi en maîtriser les risques. Ce dernier module est essentiel : la sécurité et la protection des informations conditionnent un usage professionnel serein.

Points abordés : Les principaux risques · Le risque d'injection d'instructions · La posture de fond

À retenir — Trois risques à maîtriser : confidentialité, fiabilité, sécurité des actions — plus le risque d'injection par des contenus externes. Les consignes légitimes viennent de vous ; permissions minimales, validation des actions sensibles et vérification restent vos meilleurs réflexes.

02. Exemples de situations et solutions

La théorie prend tout son sens face à des situations concrètes. Voici des cas typiques et les bons réflexes pour y répondre.

Points abordés : Situation : données sensibles à traiter · Situation : information incertaine · Situation : action irréversible proposée · Situation : contenu externe suspect

À retenir — Face aux données sensibles, à l'information incertaine, aux actions irréversibles et aux contenus suspects, les réflexes sont : limiter le partage, vérifier les faits, relire avant de valider, et ne jamais suivre des instructions cachées dans un contenu externe.

03. Règles de sécurisation de Cowork

Cowork, parce qu'il agit sur vos fichiers et peut travailler de façon autonome, appelle des règles de sécurisation spécifiques. Voici l'essentiel pour l'utiliser sereinement.

Points abordés : Maîtriser les accès et les permissions · Valider les actions à conséquence · Protéger les informations · Vérifier et superviser

À retenir — Sécuriser Cowork : minimum de permissions, validation des actions à conséquence, protection stricte des informations, et supervision humaine des livrables et des tâches automatiques. La puissance de l'agent va de pair avec votre contrôle.