SOFIA FEYZA MEISSA

NETWORK

ASSURMER

PASSWORD

* * * * * * * * *

III. Comparaison des différents protocoles de sécurité wifi

Protocole	Sécurité	Facilité d'utilisation	Utilisation actuelle
WEP	Très faible (facilement piraté)	Très simple à configurer	Obsolète, à éviter
WPA	Moyenne (amélioration de WEP, mais dépassée)	Simple à configurer	Rare, ancien réseaux
WPA2-Personal	Bonne (chiffrement AES)	Facile, basé sur un mot de passe	Très courant dans les réseaux domestiques
WPA2-Enterprise	Très bonne (serveur RADIUS)	Complexe, nécessite une configuration professionnelle	Utilisé dans les entreprises
WPA3-Personal	Excellente (protection avancée contre piratage)	Facile, avec un mot de passe	Recommandé pour les nouveaux réseaux
WPA3-Enterprise	Très excellente (chiffrement individualisé)	Complexe, adapté aux grandes organisations	Idéal pour les environnements professionnels exigeants

La sécurité Wi-Fi doit évoluer avec les menaces modernes.

WPA3 représente aujourd'hui le standard à privilégier pour tous les nouveaux réseaux. Il offre une protection robuste contre les techniques d'attaques récentes, tout en garantissant des connexions stables et sûres.

Cependant, WPA2 reste une alternative fiable pour les équipements plus anciens, surtout en mode Enterprise, où l'authentification individuelle renforce la sécurité.

Il est essentiel de privilégier des mots de passe forts pour éviter les failles.

En revanche, les protocoles comme WEP et WPA n'offrent plus un niveau de protection suffisant et doivent être abandonnés.