

WI-FI PUBLIC

ATTENTION ! VOUS ENTREZ DANS UNE ZONE DANGEREUSE



En vous connectant à un point d'accès Wi-Fi public (hôtel, restaurant, train, aéroport...), vous prenez le risque de vous faire dérober très facilement vos informations de connexion et vos données personnelles ou professionnelles. Utilisez plutôt le partage de connexion de votre téléphone lorsque c'est possible.

Il est très facile pour un pirate de créer un faux point d'accès Wi-Fi public ressemblant en tout point à un véritable point d'accès. Vous n'avez aucun moyen de vous assurer que l'accès est bien légitime et même si c'est le cas, vous n'avez aucune garantie qu'un pirate n'est pas déjà à l'écoute sur le point d'accès. Lorsque c'est possible, un partage de connexion via votre téléphone vous permettra de vous affranchir de devoir vous connecter à un point d'accès public. Si ce n'est pas possible, d'autres solutions techniques sont à envisager : mise à disposition d'un modem 4G par votre entreprise lors de vos déplacements ou installation d'un tunnel VPN vers votre entreprise afin de sécuriser les échanges lorsque vous vous connectez sur un accès public.



CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information