La Cyber-Lettre
de la
GENDARMERIE
RÉGION GRAND EST

Février 2026

🕵️ L'attaque Man-in-the-Middle (MIM)

" l'homme du milieu "

DIFFUSION LIBRE

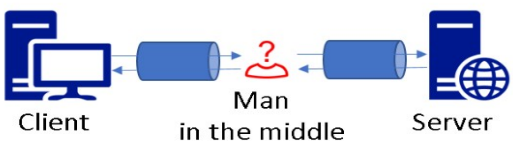
Une attaque Man In The Middle se produit lorsqu'un pirate s'interpose discrètement entre deux personnes 🦹 ou deux systèmes qui communiquent. Par exemple entre un utilisateur et un site internet, un téléphone et un réseau Wi-Fi ou encore une application et son serveur.

L'attaquant 🎭 intercepte les informations échangées, peut les écouter, les lire, les modifier ou les voler, sans que la victime ne s'en rende compte. Un peu comme si quelqu'un écoutait une conversation téléphonique ou ouvrait votre courrier avant qu'il n'arrive.

Ainsi, toutes les données sensibles telles qu'identifiants et mots de passe, numéros de carte bancaire, messages privés ou encore données professionnelles transitent par le pirate. Ce dernier peut aisément espionner, recevoir, modifier les messages ou rediriger vers de faux sites.🫣

Les attaques Man In The Middle sont particulièrement courantes sur les Wi-Fi publics gratuits *(gares, cafés, hôtels, aéroports)*, les réseaux non sécurisés ou mal configurés ou lors de connexions à des sites non chiffrés *(HTTP au lieu de HTTPS)*.

Les risques pour les victimes sont principalement le vol de mots de passe, l'usurpation d'identité, le piratage de comptes *(mail, réseaux sociaux, banque)*, l'espionnage de données ou le vol d'argent 💰 *(modification d'un RIB par exemple)*



💡 Bon à savoir :

Un appel téléphonique de sûreté avant de valider une opération n'est jamais superflux

Un Wi-Fi gratuit n'est jamais gratuit. S'il ne coûte rien, c'est parfois vos données qui le paient.

Les attaques peuvent viser aussi bien les particuliers que les entreprises ou les collectivités.

🛡️ Comment se protéger ?

✅ Activer une authentification à deux facteurs dite « 2FA » ;

✅ Éviter les Wi-Fi publics pour réaliser des opérations sensibles *(banque, achats en ligne, messagerie pro)* ;

✅ Vérifier systématiquement la présence du HTTPS *(protocole sécurisé)* et du cadenas (🔒) dans la barre d'adresse ;

✅ Utiliser un VPN de confiance lors de connexions nomades ;

✅ Mettre à jour régulièrement ses appareils et applications ;

✅ Ne jamais ignorer une alerte de certificat de sécurité ;

✅ Privilégier le partage de connexion mobile plutôt qu'un Wi-Fi inconnu.

Vous êtes victime ?

Appelez immédiatement le 📞**17** ou 💻 contacter :

LE 17 CYBER

Une cyberattaque, échangez avec un cybergendarme - 24h/24 7j/7
https://17cyber.gouv.fr/

GRAND EST CYBERSECURITE

Assistance cyberattaque gratuite
Tel : 0 970 512 525
www.cybersecurite.grandest.fr

+ D' INFO

LA CNIL

Prévenir en cas de fuite de données personnelles, réelle ou supposée.

CYBERMALVEILLANCE

Pour vous faire assister, vous informer ou vous former
www.cybermalveillance.gouv.fr

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

L'ANSSI

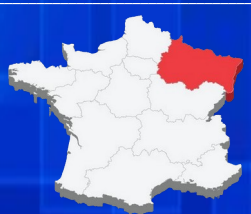
Assiste les entités essentielles et les entités importantes, fournit des guides
https://cyber.gouv.fr

THÉSÉE

Déposer plainte en ligne pour les victimes d'e-escroqueries

APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.



Vous souhaitez joindre un Référent Cyber de la Région de Gendarmerie du Grand-Est ou vous abonner à la Cyber-lettre
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)

01010010 01001001 01010011 01000011 01001000