La Cyber-Lettre
de la
GENDARMERIE
RÉGION GRAND EST

Mars 2026

Le spoofing

L'usurpation de numéro de téléphone.

DIFFUSION LIBRE

Le spoofing est une technique d'arnaque qui consiste à se faire passer pour une personne, une entreprise ou un tiers de confiance afin de tromper une victime.

Le fraudeur 🦹 cherche à imiter une identité légitime *(banque, administration, service de livraison, etc)* en donnant l'illusion que le message ou l'appel reçu est authentique.

Pour ce faire il utilise des applications spécifiques qui permettent d'afficher un numéro d'appel connu 📞ou une adresse mail quasi identique à celle d'un organisme officiel.

Le cyberdélinquant tente d'instaurer un climat de confiance *(souvent accompagné d'un sentiment d'urgence ou de peur)* afin de pousser la victime à agir rapidement sans prendre le temps de vérifier.

L'objectif final est toujours le même, obtenir des informations sensibles, de l'argent ou un accès à des comptes bancaires personnels ou professionnels 🏦. En voici deux exemples :

- De nombreux clients d'établissements bancaires ont été victimes de cette fraude. Ils ont reçu des appels frauduleux affichant le véritable numéro du service client. Rassurés par cet affichage, ils communiquent leurs codes de validation ou leurs informations bancaires.

➡️ Des milliers de victimes, des comptes vidés en quelques minutes

- Les cybermalfaiteurs appellent en se faisant passer pour l'assurance maladie, prétextant une mise à jour de dossier ou un remboursement. Le numéro affiché correspond à la plateforme officielle.

➡️ Vol de données personnelles, puis fraudes en cascade. 🎭

💡 Bon à savoir :

➡️ Le numéro affiché n'est pas toujours une preuve d'identité ;

➡️ Les cybermalfaiteurs peuvent falsifier l'affichage du numéro (caller ID spoofing) ;

➡️ Un mail peut sembler légitime alors qu'il provient de l'étranger ;

➡️ Les attaques de spoofing sont souvent le point d'entrée d'arnaques plus complexes *(fraude au président, vishing et smishing – hameçonnages voix et sms)*

🛡️ Comment se protéger ?

✅ Activer l'authentification à deux facteurs *(2FA)* sur tous les comptes importants
✅ Ne jamais cliquer sur un lien reçu sans vérification
✅ Ne jamais communiquer vos codes, mots de passe ou coordonnées bancaires
✅ En cas de doute, raccrocher et rappeler le numéro officiel connu
✅ Sensibiliser les équipes et les proches à ce type de fraude

Vérifier une information peut suffire à éviter une arnaque aux conséquences lourdes

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/

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

+ 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

GRAND EST CYBERSECURITE

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

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