



La Cyber-Lettre de la **GENDARMERIE** **RÉGION GRAND EST**



Mois 2026

Les pixels transparents : l'espion invisible dans vos e-mails



Un pixel transparent 🧑🏻 est une image invisible de 1 x 1 pixel, hébergée sur un serveur distant. Lorsque votre logiciel de messagerie affiche automatiquement les images du message, il télécharge ce pixel. Cette simple requête informe alors le serveur que le message a été ouvert.

Pour l'utilisateur, rien n'apparaît à l'écran, pour l'expéditeur, de nombreuses informations sont collectées.

Les pixels transparents sont largement utilisés dans le marketing pour mesurer l'efficacité des campagnes d'e-mails. Cependant, ils peuvent également être exploités à des fins malveillantes.

🕵️ Un cybercriminel peut ainsi :

- vérifier qu'une adresse e-mail est active ;
- identifier les personnes les plus susceptibles de lire rapidement leurs messages ;
- adapter une campagne de phishing en fonction de votre comportement ;
- confirmer qu'une cible est présente dans une entreprise ;
- recueillir des informations techniques utiles pour préparer une attaque.

Un simple e-mail devient alors un véritable outil de reconnaissance.

Imaginez, une entreprise 🏢 qui reçoit un faux message se faisant passer pour un transporteur. Le destinataire ne clique sur rien et pense être en sécurité. Pourtant, l'ouverture du message déclenche le chargement du pixel transparent.

Le pirate sait désormais :

- que l'adresse est valide ;
- que le salarié consulte régulièrement sa messagerie ;
- à quel moment il est généralement connecté.

Quelques jours plus tard, la même entreprise reçoit un second e-mail de phishing beaucoup plus crédible, envoyé au moment où elle consulte habituellement ses messages.



Comment se protéger ?

Quelques bonnes pratiques permettent de limiter ce pistage :

- désactiver le chargement automatique des images dans votre messagerie ;
- privilégier l'affichage des images uniquement pour les expéditeurs de confiance ;
- rester vigilant face aux e-mails inattendus, même sans pièce jointe ;
- sensibiliser les collaborateurs à cette technique souvent méconnue.

À retenir

L'absence de clic ne signifie pas l'absence de collecte d'informations. Aujourd'hui, ouvrir un e-mail peut suffire à révéler des informations précieuses sur votre activité numérique.

Dans le domaine de la cybersécurité, la phase de reconnaissance est souvent la première étape d'une attaque. Les pixels transparents en sont l'un des outils les plus discrets... et les plus efficaces.

Le conseil du Référent Cyber de la Gendarmerie

Restez vigilant : avant même de cliquer sur un e-mail, interrogez-vous sur les données qu'il pourrait collecter à votre insu.

La meilleure défense reste la vigilance.

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



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**
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)



01010010 01001001 01010011 01000011 01001000