

Se protéger des « pixels de suivi » et du pistage dans les courriels

Qu'est-ce qu'un pixel de suivi ?

Un pixel de suivi est une image minuscule, souvent invisible (1 × 1 pixel), intégrée dans un courrier électronique au format HTML.

Lorsque votre logiciel de messagerie affiche ce message, il peut être amené à télécharger cette image depuis le serveur de l'expéditeur. Ce simple téléchargement lui permet de savoir que le message a été ouvert.

L'expéditeur peut ainsi obtenir des informations telles que :

- la date et l'heure de l'ouverture du message ;
- le nombre de fois où il a été ouvert ;
- votre adresse IP (ou celle d'un serveur intermédiaire) ;
- parfois le logiciel de messagerie ou le système d'exploitation utilisés.

Pourquoi certains courriels vous espionnent-ils ?

De nombreux courriels commerciaux contiennent un **pixel de suivi**. Il s'agit d'une image minuscule, invisible à l'œil nu, intégrée dans le message.

Lorsque vous ouvrez ce courriel, votre logiciel ou votre navigateur peut télécharger cette image depuis le serveur de l'expéditeur. Celui-ci sait alors que le message a été ouvert et peut également recueillir diverses informations, par exemple :

- la date et l'heure de l'ouverture ;
- le nombre de consultations du message ;
- votre adresse IP (ou celle d'un serveur intermédiaire) ;
- parfois le logiciel ou le navigateur utilisé.

Cette technique est largement employée dans les campagnes publicitaires et les lettres d'information.

Le principal problème : le webmail

Aujourd'hui, beaucoup de personnes consultent leur courrier directement dans un navigateur Web (Gmail, Outlook.com, Yahoo Mail, Orange, Free, SFR, etc.). C'est ce qu'on appelle un **webmail**.

Or un webmail affiche les messages sous forme de pages Web. Le contenu HTML est interprété par le navigateur, ce qui facilite le chargement des images distantes utilisées pour le pistage.

Certains fournisseurs mettent en place des protections, mais celles-ci varient selon les services et ne suppriment pas toutes les possibilités de suivi. L'utilisateur dépend entièrement des choix du fournisseur.

Une solution plus sûre : utiliser un logiciel de messagerie

Il est préférable de consulter son courrier avec un **logiciel de messagerie** installé sur son ordinateur, appelé aussi **client de messagerie**.

Quelques exemples :

- Mozilla Thunderbird (logiciel libre) ;
- Microsoft Outlook ;
- Apple Mail ;
- Evolution (Linux).

Avec un logiciel dédié, vous gardez la maîtrise de nombreux réglages de sécurité et de confidentialité.

Le cas de Thunderbird

Thunderbird offre des protections particulièrement efficaces lorsqu'il est correctement configuré.

Les réglages recommandés sont les suivants :

- afficher les messages en **texte brut** plutôt qu'en HTML ;
- désactiver le chargement automatique des contenus distants ;
- ne jamais envoyer automatiquement les accusés de lecture.

Dans cette configuration, les pixels de suivi classiques ne peuvent pas être téléchargés.

Rester prudent

Même avec ces protections, un lien contenu dans un message peut comporter un identifiant unique. En cliquant dessus, vous signalez au site visité que vous avez utilisé ce lien.

Il est donc conseillé de ne cliquer que sur les liens provenant d'expéditeurs de confiance et lorsque cela est réellement nécessaire.

En résumé

Pour mieux protéger votre vie privée :

- évitez autant que possible de consulter votre courrier uniquement avec un webmail ;
- préférez un véritable logiciel de messagerie installé sur votre ordinateur ;
- si vous utilisez Thunderbird, affichez les messages en texte brut et bloquez le chargement des contenus distants ;
- n'envoyez pas automatiquement les accusés de lecture ;
- soyez prudent avec les liens contenus dans les courriels.

Ces quelques précautions réduisent fortement les possibilités de pistage et permettent de reprendre le contrôle de votre messagerie.