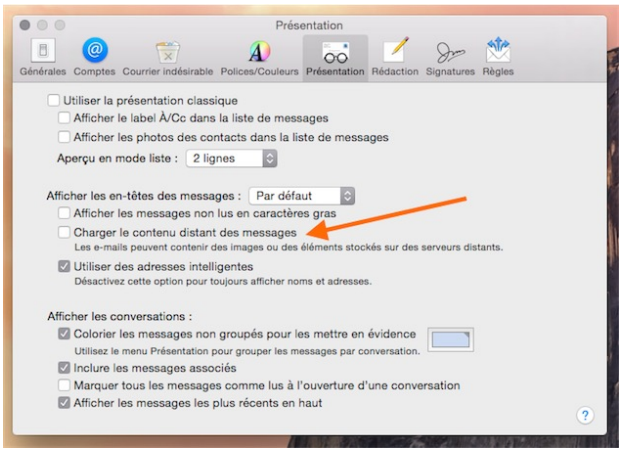
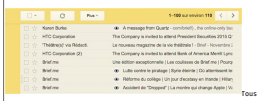
Comment se protéger des emails trop curieux | Denis JACOPINI



Comment se protéger des emails trop curieux

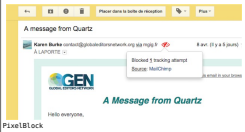
Sans même que vous visitiez un site web, les publicitaires peuvent récolter des informations vous concernant. L'une des techniques utilisées, très répandue et pas illégale, est le pixel tracking.

Une image transparente de 1 x 1 pixel liée à une URL est insérée dans un email. Quand l'email est ouvert, cette minuscule image est chargée et communique avec les serveurs du publicitaire qui a alors accès à des données personnelles, comme l'adresse IP, l'emplacement géographique (via l'IP), l'heure de la consultation et le terminal utilisé.
Les éditeurs ne font pas toujours preuve de tant de discrétion pour récolter des informations à partir des emails (une simple image, comme un logo d'entreprise, suffit), mais le résultat est le même ; des données sont récoltées sans le consentement de l'utilisateur.



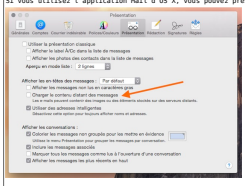
Tous les éditeurs n'utilisent pas le pixel tracking ou une autre technique de traçage à des fins publicitaires. Brief.me, un mini-journal disponible uniquement par email, l'exploite par exemple pour avoir des statistiques de consultation.

L'extension Chrome UglyEmail met en lumière les emails exploitant des techniques de traçage d'entreprises spécialisées (Streak, Yesware, Mandrill, MailChimp, Postmark, TinyLetter, Sidekick, MixMax et Bananatag). Quand UglyEmail repère dans la boîte de réception de Gmail un email trop curieux, il le signale avec une petite icône d'œil.
L'extension n'enregistre et ne transmet aucune donnée provenant de Gmail, assure son auteur à Wired. Des versions pour Firefox et Safari sont en développement.
PixelBlock, une autre extension Chrome réservée elle aussi à Gmail, va plus loin puisqu'elle bloque carrément le tracking. En cliquant sur l'œil rouge à côté du nom de l'expéditeur, on découvre la source du service de traçage.



PixelBlock

Si vous utilisez l'application Mail d'OS X, vous pouvez préserver votre confidentialité en désactivant le chargement des contenus distants des emails (l'option se trouve dans l'onglet Présentation des préférences). Cela fonctionne avec tous les fournisseurs de courrier électronique (Gmail, iCloud, Outlook, Yahoo…).



Puisque le lien avec le serveur distant est coupé, les informations personnelles ne sont pas divulguées. Cela a aussi pour effet de « casser » la mise en page des emails qui utilisent des images distantes, mais Mail permet très simplement de charger le contenu distant au cas par cas (un bouton est présent en haut du courrier quand le cas se présente).

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.macg.co/logiciels/2015/04/confidentialite-comment-se-proteger-des-emails-trop-curieux-88326
Par Stéphane Moussie