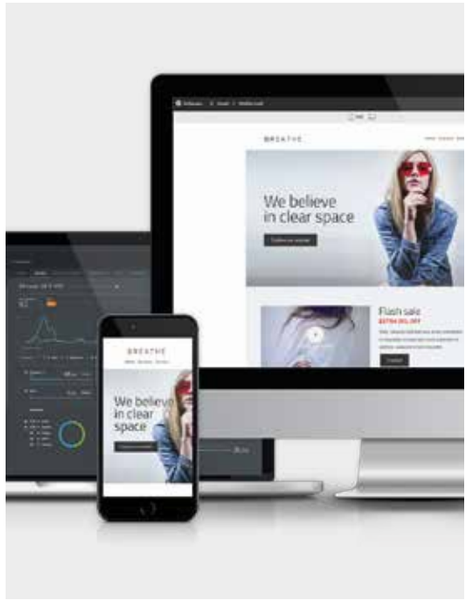
PAROLES D'EXPERTS

Pierre GALIÈGUE,
Responsable Délivrabilité chez Sarbacane Software

Comprendre les normes d'authentification permet d'assurer une bonne délivrabilité emailing

SPF, DKIM, DMARC et désormais BIMI, ces acronymes aux noms « barbares » révèlent une autre facette de l'emailing : les normes d'authentification. Car si le respect du RGPD, la bonne segmentation des bases, la pertinence des messages restent des pré-requis, le respect des règles d'authentification permet de certifier l'identité d'un expéditeur, et ainsi améliorer la réputation.



Sarbacane

Quand on sait que près d'un email sur 4 est considéré comme du spam, l'enjeu est de taille.
Voici un tour d'horizon des normes d'authentification en vigueur.

SPF (SENDER POLICY FRAMEWORK) : EST-CE QUE LE SERVEUR EST AUTORISÉ À ÉMETTRE DES EMAILS POUR CE DOMAINE ?

Le SPF est un système de validation des IP expéditrices d'un courriel dont le rôle est d'empêcher les spammeurs d'envoyer des messages au nom de votre domaine.
Cet enregistrement spécifie les adresses IP et/ou les noms d'hôtes autorisés à envoyer des e-mails à partir du domaine spécifique. Ainsi, le destinataire pourra vérifier depuis l'adresse *« FROM »* du courrier que l'adresse IP d'envoi a été autorisée à le faire. A contrario, lorsque le serveur de courrier électronique expéditeur n'est pas inclus dans le SPF d'un domaine spécifique, la messagerie peut décider de traiter ce message comme un courrier indésirable.

DKIM (DOMAINKEYS IDENTIFIED MAIL) : VÉRIFICATION DE LA CORRESPONDANCE ENTRE SIGNATURE ET CLÉ PUBLIQUE

Le DKIM donne aux courriels une en-tête de signature qui est ajoutée au message, et sécurisée par un cryptage. Cette signature DKIM fait office de sceau inviolable pour le courrier électronique afin de vérifier qu'il provient bien du domaine indiqué et qu'il n'a pas été altéré. Le serveur email d'origine possède ce que l'on appelle une *« private key » (clé DKIM privée), qui peut être vérifiée par la messagerie du destinataire avec l'autre moitié de la paire de clés, appelée « public key »* (clé DKIM publique).

Le sélecteur DKIM se trouve dans l'en-tête de la signature DKIM et indique où se trouve la partie publique de la paire de clés dans le DNS.
L'implémentation de DKIM pour la messagerie électronique présente 3 grands avantages : la protection de l'intégrité des messages (il est possible de vérifier que le contenu du courriel n'a pas été modifié pendant la transmission), l'augmentation de la réputation du domaine et la délivrabilité des courriels, et une méthode fondamentale de vérification des emails pour DMARC.

DMARC (DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE) : ENVOI D'UN FEEDBACK

Le DMARC est une spécification technique qui permet de vérifier l'authenticité d'un courriel en complétant les spécifications SPF et DKIM. Justement, le DKIM et le SPF n'ont pas de notion d'alignement des domaines (c'est-à-dire que le même domaine envoie et *« signe »* le message).
Le DMARC permet de lutter contre la fraude BEC (Business Email Compromise), l'usurpation d'identité et les attaques d'hameçonnage. Il améliore par ailleurs la délivrabilité.

BIMI (BRAND INDICATORS FOR MESSAGE IDENTIFICATION) : LE PETIT NOUVEAU

Le BIMI est un standard qui facilite l'identification de l'émetteur d'un courriel.
Il coordonne les messageries et les propriétaires de noms de domaine pour permettre à ces derniers d'afficher leurs logos directement au niveau de la boite e-mail de leurs clients (à côté du nom de l'émetteur). Bien que le BIMI ne soit pas encore largement adopté par les messageries, il permet une meilleure visibilité de la marque et de réaffirmer l'authenticité de celle-ci chez certaines messageries.
Les FAI utilisent l'authentification pour protéger les destinataires des emails indésirables et non sécurisés. Cependant, même des messages légitimes peuvent parfois être filtrés. C'est pourquoi les entreprises et communicants se doivent de connaître le fonctionnement de ces normes pour se protéger et par la même occasion, assurer une bonne délivrabilité de leurs emails.