

Dolist renforce la sécurité de ses envois e-mails en adoptant le protocole TLS

Dolist adopte de manière précurseur le tout dernier protocole de sécurité des envois e-mail marketing et renforce ainsi la sécurité des données de ses clients.

Bordeaux, le 26 mars 2015 - Afin de protéger davantage les routages des communications e-mails de ses clients et les échanges avec ces derniers, Dolist a implémenté le plus solide protocole de sécurité actuel (TLS - Transport Layer Security) pour tous les messages envoyés depuis les technologies Dolist et les transmissions de données vers celles-ci.

TLS, le protocole de cryptage sécurisé nouvellement préconisé

L'industrie de l'e-mail marketing s'est appuyée pendant des années sur le protocole de sécurisation des échanges sur le Web nommé SSL (Secure Sockets Layer). Celui-ci a cependant récemment été remis en cause suite à des faiblesses de sécurité affectant les données contenues dans les messages pendant leur acheminement.

Le M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group), le groupe international de lutte contre le spam œuvrant pour la protection des internautes qui fédèrent les acteurs de l'industrie e-mail, vient de recommander à tous ses membres de **privilégier le protocole de chiffrement TLS**. Celui-ci a été créé en 1999 pour pallier aux faiblesses du SSL mais fut pourtant peu implémenté jusque-là.

Une nouvelle norme de sécurité pour les messageries

Le protocole TLS permet une véritable **protection des données échangées pendant leur transport** par e-mail. Le but est d'empêcher l'interception et le vol des données par quelqu'un ayant, par exemple, accès au réseau sur lequel elles sont transportées. L'intérêt de cette protection est par ailleurs accru dans le cadre d'envoi d'e-mails transactionnels qui peuvent facilement contenir des données personnelles confidentielles.

Suite aux recommandations du M3AAWG, la plupart des grands fournisseurs de messagerie l'ont ou vont bientôt le mettre en œuvre. Leurs objectifs sont de limiter les risques liés aux messages piratés et de protéger toujours davantage les internautes de telles menaces. **Ce protocole va ainsi devenir la norme de toute messagerie sécurisée.**

La délivrabilité des campagnes des annonceurs impactée

Au-delà de ces aspects sécuritaires, la délivrabilité des messages e-mails des annonceurs va également être impactée. En effet, des fournisseurs de messagerie comme Google ont clairement confirmé **favoriser à l'avenir la livraison de messages protégés** pendant leur transport vers les serveurs Gmail par le protocole TLS.

« Une protection renforcée des échanges de données via le canal e-mail devient aujourd'hui indispensable. C'est pourquoi **nous avons adopté ce protocole pour l'ensemble de nos technologies**, rejoignant l'ensemble de nos solutions techniques visant à assurer la sécurité des opérations marketing et la réputation de nos clients. Ces derniers doivent pouvoir s'appuyer sur un prestataire de confiance en s'assurant que **les informations qu'ils intègrent dans leurs messages ne peuvent être dérobées** et utilisées à des fins frauduleuses », conclut Denis Olivier, directeur associé en charge de la technologie de Dolist.

À propos de Dolist

Dolist, spécialiste Data & E-mail Marketing depuis 2000, propose des services de production, d'audit, de consulting, d'accompagnement et de formation dans le domaine du Data Driven Marketing. Objectif : permettre aux professionnels d'optimiser leurs dispositifs digitaux pour accroître le ROI de leurs campagnes.

En parallèle, Dolist fournit des technologies d'envoi d'e-mails, de SMS et d'e-mails transactionnels facilitant l'acquisition, l'enrichissement et l'exploitation de données (scoring, personnalisation, automatisation, analytics...).

Informations et actualités : www.dolist.net

Contact presse

Gaëlle Guillocheau, responsable communication

g.guillocheau@dolist.net

06 58 35 43 10