Pôle Activ'Océan
9 Rue de Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

Sécurité avancée de votre messagerie

PREAMBULE

La sécurité de la messagerie de l'entreprise est une priorité qu'il ne faut surtout pas négliger. Non seulement il est important **d'éviter que votre messagerie soit vectrice de piratage** de votre entreprise mais aussi qu'elle ne **mette en danger vos contacts**. En effet, il est de plus en plus courant que des cybers criminels usurpent une identité afin d'escroquer des clients, partenaires et collaborateurs en utilisant l'abus de confiance. Bien entendu, le minimum vital est de sauvegarder votre messagerie, de vous **équiper d'un anti-spam et d'un antivirus performant**. Cependant ce n'est pas suffisant. Il est capital de paramétrer votre messagerie suivant des règles de cyber sécurité pointues.

Nos équipes cyber et spécialistes de la messagerie sont en mesure de vous assister.
Voici quelques explications :

❖ SPF (Sender Policy Framework)

Mettre en place SPF (Sender Policy Framework) est essentiel pour améliorer la sécurité et la délivrabilité des emails envoyés par votre domaine. Voici quelques raisons pour lesquelles il est important d'implémenter SPF :

- Lutte contre l'usurpation d'identité (spoofing) : SPF aide à protéger votre domaine contre les usurpateurs qui pourraient envoyer des emails frauduleux en utilisant votre nom de domaine dans l'enveloppe "MAIL FROM". En mettant en place SPF, vous indiquez aux serveurs de messagerie des destinataires quels serveurs sont autorisés à envoyer des emails en votre nom, réduisant ainsi la probabilité d'usurpation d'identité.

- Amélioration de la délivrabilité des emails : Les serveurs de messagerie des destinataires vérifient souvent l'enregistrement SPF du domaine de l'expéditeur pour s'assurer que l'email provient d'une source autorisée. Si vous avez un enregistrement SPF valide, vos emails ont de meilleures chances d'être acceptés et de ne pas être considérés comme du spam ou du phishing.

- Réputation du domaine : Un domaine qui a mis en place SPF est perçu comme plus fiable par les serveurs de messagerie et les fournisseurs de services de messagerie. Cela peut contribuer à améliorer la réputation de votre domaine, ce qui est essentiel.

❖ DKIM (DomainKeys Identified Mail)

Mettre en place DKIM (DomainKeys Identified Mail) est important pour renforcer la sécurité et la délivrabilité des emails envoyés par votre domaine. Voici quelques raisons pour lesquelles il est essentiel d'implémenter DKIM :

- Authentifier l'expéditeur : DKIM permet aux destinataires de vérifier que l'email provient réellement du domaine prétendu. Les serveurs de messagerie et les fournisseurs de services sont plus enclins à accepter les emails authentifiés, car cela réduit les risques d'usurpation d'identité, de phishing et d'autres types de fraudes.

- Préserver l'intégrité du message : La signature DKIM garantit que le contenu de l'email n'a pas été modifié en cours de route. Les serveurs de messagerie sont plus susceptibles de livrer des emails dont l'intégrité est vérifiable, car cela permet d'assurer que les messages ne contiennent pas de contenu malveillant ou frauduleux.

- Améliorer la réputation du domaine : L'utilisation de DKIM renforce la réputation de votre domaine en montrant que vous prenez des mesures pour protéger vos emails contre les abus et les usurpations. Une bonne réputation de domaine est cruciale pour la délivrabilité des emails, car les serveurs de messagerie et les fournisseurs de services tiennent compte de cette réputation lorsqu'ils évaluent les emails entrants.

❖ DMARC (Domain-based Message Authentication, Reporting, and Conformance Haut du formulaire)

DMARC (Domain-based Message Authentication, Reporting, and Conformance) est un protocole de sécurité pour les emails qui vise à lutter contre l'usurpation d'identité (spoofing) et d'autres types de fraudes par email. DMARC repose sur les mécanismes d'authentification DKIM (DomainKeys Identified Mail) et SPF (Sender Policy Framework) et permet aux propriétaires de domaines de spécifier comment les destinataires doivent gérer les emails qui échouent à ces vérifications d'authentification.

En somme, « Sapiens: Une brève histoire de l'humanité » est un livre qui explore l'histoire de l'humanité depuis ses origines jusqu'à aujourd'hui, en analysant les grandes révolutions qui ont marqué l'évolution de notre espèce.

Confiez-nous votre sécurité ! Consultez-nous

Pôle Activ'Océan
9 Rue de Bois Fossé - BP 147
85301 CHALLANS Cedex

Tél. : 02 51 49 31 31
Email : contact@espace-technologie.com
Web : www.espace-technologie.com

Organisme de formation n° 52850059385 - SAS au capital de 38 500 € - Siret : 38979357100024 - APE : 4741Z - RCS La Roche sur Yon B389793571