AXION.

Rapport de sécurité — abaxinfo.com

Revue passive du site web, de la messagerie et du nom de domaine

Destinataire : Eric — ABAXINFO
Émis par : AXION — Djemel Chaouche
Date : 1er juillet 2026
Périmètre : site `www.abaxinfo.com`, configuration email, nom de domaine `abaxinfo.com`
Nature : revue **passive et non-intrusive** — analyse de données publiques, sans aucune attaque ni test d'intrusion

1. Synthèse pour décision

Le niveau de sécurité d'ABAXINFO est **globalement sain**. Aucune faille critique exploitable n'a été détectée sur le site web, et les protections de base du nom de domaine sont en place.

Il reste **deux actions à réelle valeur** :

1. **Renforcer la protection anti-usurpation des emails** (protocole DMARC, aujourd'hui en mode « surveillance seule » : il observe mais ne bloque rien). En l'état, un fraudeur peut envoyer un email en se faisant passer pour une adresse `@abaxinfo.com`.
2. **Activer la double authentification (2FA)** sur les comptes clés et **signer le domaine (DNSSEC)** — des durcissements simples et rapides.

Aucune action n'est urgente au sens « incident en cours », mais la première (DMARC) protège contre la fraude par email, aujourd'hui le risque n°1 des PME.

Chaque terme technique est défini à sa première apparition, afin de rester lisible sans expertise informatique.

2. Contexte technique

Le site `www.abaxinfo.com` est hébergé sur **Wix**, une plateforme « managée » : entretien du serveur, correctifs, chiffrement et protection contre les attaques de saturation sont assurés par Wix. Cela réduit fortement la surface de risque — pas de logiciel serveur à maintenir soi-même (pas de WordPress ni de base de données auto-hébergée).

Les emails sont gérés via **Microsoft 365** (messagerie Outlook), avec une passerelle anti-spam **Mailinblack** en amont pour filtrer le courrier entrant.

Le nom de domaine `abaxinfo.com` est enregistré chez **Gandi** (le « registrar », organisme auprès duquel le domaine est loué), qui héberge aussi la zone DNS — le DNS (*Domain Name System*) étant l'annuaire qui traduit `abaxinfo.com` en adresses techniques.

3. Résultats détaillés

3.1 Site web

Élément vérifié	Résultat	Évaluation
Redirection automatique vers HTTPS	Oui	✅ **Conforme**
HSTS — *HTTP Strict Transport Security* (force le navigateur à toujours chiffrer la connexion)	Activé (~1 an)	✅ **Conforme**
Certificat TLS — *Transport Layer Security* (le « cadenas » du navigateur)	Valide (renouvellement auto)	✅ **Conforme**
Protection anti-détournement de type de fichier	Activée	✅ **Conforme**
Exposition de fichiers sensibles (config, sauvegardes, code)	Aucune — tous bloqués	✅ **Conforme**
Interface d'administration WordPress attaquable	Absente (pas de WordPress)	✅ **Conforme**
En-tête CSP — *Content Security Policy* (limite les scripts exécutables)	Absent	⚠️ **Limite Wix**
Protection anti-« clickjacking »	Absente	⚠️ **Limite Wix**

Lecture : les fondamentaux sont respectés. Les en-têtes manquants **ne sont pas des négligences** : la plateforme Wix ne permet pas d'ajouter ces en-têtes personnalisés. Pour un site vitrine, le risque associé est faible.

3.2 Configuration email

Trois mécanismes standard protègent contre l'usurpation d'identité par email :

Mécanisme	Rôle	État actuel	Éval.
SPF Sender Policy Framework	Liste les serveurs autorisés à envoyer au nom du domaine	Présent (Microsoft 365, Mailgun, Autotask, SiPortal), mode « souple »	⚠️
DKIM DomainKeys Identified Mail	Signe chaque email pour prouver son authenticité	Présent (deux signatures actives)	✅
DMARC Domain-based Message Authentication	Décide quoi faire d'un email suspect et produit des rapports	Présent mais réglé sur « surveillance seule » (aucun blocage)	🔴

> **Point d'attention principal — DMARC en « surveillance seule ».** Le réglage actuel collecte des rapports mais **n'empêche pas** la livraison d'emails frauduleux usurpant le domaine. Un tiers malveillant peut aujourd'hui envoyer un email paraissant provenir de `@abaxinfo.com` (fausse facture, « fraude au président ») sans qu'il soit automatiquement rejeté. C'est le principal levier d'amélioration.

Point secondaire — SPF : la configuration autorise quatre sources d'envoi. Le protocole SPF est limité à 10 vérifications techniques ; au-delà, il cesse de fonctionner silencieusement. Il conviendra de vérifier qu'on reste sous cette limite lors de la mise en œuvre.

3.3 Nom de domaine

Élément vérifié	Résultat	Évaluation
Verrouillage anti-transfert (empêche le vol du domaine)	Activé	✅ **Conforme**
Date d'expiration	23 mars 2027	✅ **Marge confortable**
DNSSEC — *DNS Security Extensions* (signe l'annuaire DNS contre la falsification)	Non activé	⚠️ **À activer**

Lecture : le verrou anti-transfert — la protection domaine la plus importante — est déjà en place, ce qui écarte le risque de détournement du nom de domaine. Il reste à activer la signature DNSSEC.

4. Plan d'action recommandé

Actions classées par rapport valeur / effort. Aucune ne présente de risque de coupure si elle est menée dans l'ordre indiqué.

Action 1 — Renforcer DMARC (priorité haute, sans coût)

Passage **progressif** en trois paliers, sur ~6 semaines, pour ne jamais bloquer un email légitime. Un seul enregistrement DNS à modifier chez Gandi.

1. **Palier 1 (immédiat) :** mise en quarantaine de 25 % des emails suspects.
2. **Palier 2 (après ~3 semaines de vérification) :** quarantaine de 100 %.
3. **Palier 3 (après ~3 semaines supplémentaires) :** rejet total des emails usurpant le domaine.

Entre chaque palier, les rapports DMARC (déjà envoyés à `global.admin@abaxinfo.com`) sont analysés pour vérifier que tous les expéditeurs légitimes passent les contrôles. AXION fournit le texte exact de chaque enregistrement et accompagne la lecture des rapports.

Action 2 — Double authentification + DNSSEC (priorité haute, rapide)

- **Double authentification (2FA — connexion en deux étapes)** sur les trois comptes qui contrôlent tout : **Gandi** (domaine et DNS), **Microsoft 365** (messagerie), **Wix** (site

web). Un compte administrateur compromis reste le premier vecteur d'attaque, avant toute faille technique.

- **DNSSEC** à activer chez Gandi : simple réglage, sans interruption, car Gandi héberge déjà le DNS et gère les clés automatiquement.

Action 3 — Vérifications de confort (priorité basse)

- Confirmer que la configuration SPF reste sous la limite des 10 vérifications.
- Envisager à terme un durcissement du SPF (mode strict), une fois DMARC pleinement en place.

5. Conclusion

ABAXINFO présente une posture de sécurité **saine et sans faille critique** : hébergement managé bien tenu, chiffrement correct, domaine verrouillé, signatures email en place. Les deux chantiers recommandés — **renforcement DMARC** et **double authentification + DNSSEC** — sont peu coûteux, sans risque de coupure, et couvrent le risque le plus réaliste pour une PME aujourd'hui : la fraude et l'usurpation par email.

AXION reste disponible pour mettre en œuvre ces actions et vérifier leur bonne prise en compte après déploiement.

Ce rapport résulte d'une analyse passive de données publiques. Il ne constitue pas un test d'intrusion, lequel nécessiterait un mandat écrit distinct. — AXION · axion.supply