Voici une analyse des serveurs de mail d'un point de vue sécurité/confidentialité, notamment entre ceux gérés par des FAI français et des services spécialisés "privacy / encryptés", suivie d'un classement comparatif du "moins sûr" au "plus sûr". On peut aussi discuter s'il vaut mieux choisir un serveur non affilié à un FAI.

Ce qui compte pour la sécurité d'un serveur de mail

Avant tout, voici les critères principaux qui déterminent le niveau de sécurité / confidentialité :

1. **Chiffrement en transit** — TLS, chiffrement des SMTP/IMAP/POP entre toi et le serveur, et entre serveurs.
2. **Chiffrement au repos (storage)** — les données stockées (mails, pièces jointes) doivent être chiffrées, idéalement de façon que seul l'utilisateur puisse les déchiffrer (chiffrement de bout en bout ou "zero-access").
3. **Authentification forte** — mots de passe robustes, idéalement 2-facteurs, possibilité d'avoir des mots de passe dédiés aux applications, etc.
4. **Protection contre le spam / phishing / usurpation (spoofing)** — protocoles comme SPF, DKIM, DMARC, vérification des certificats, DANE, DNSSEC.
5. **Respect de la vie privée / juridiction** — où sont situés les serveurs, quelles lois s'appliquent, s'il y a des obligations légales de fournir des données aux autorités.
6. **Transparence / audits / open source** — si le service publie des audits de sécurité ou est partiellement open source, cela augmente la confiance.
7. **Politiques de sauvegarde, redondance, réponse aux incidents** — fiabilité, capacité à résister à des attaques, à des défaillances, etc.

Sécurité des serveurs des FAI français

Les FAI (Orange, SFR, Bouygues, Free, etc.) assurent divers niveaux de sécurité / protection. Voici ce qu'on sait, et ce qu'on peut légitimement douter :

Ce qu'on sait

- Orange, par exemple, met en place des mesures pour renforcer l'accès aux boîtes mails : mot de passe dédié pour les accès depuis des clients externes / applications, authentification renforcée, etc. Assistance Orange
- Ces FAI doivent respecter le droit français / européen (RGPD notamment) et les obligations sur le secret des correspondances, etc. messagerie Orange+1
- Orange a aussi un "CERT" / centre de réponse aux incidents, effectuant des scans, surveillant les vulnérabilités, etc. Orange

Ce qu'on peut douter ou qui pose problème

- **Chiffrement de bout en bout** : les boîtes mails des FAI ne proposent généralement pas de chiffrement où seul l'utilisateur contrôle la clé (PGP ou équivalent). Le service stocke souvent les données en clair ou chiffrées mais avec des clés accessibles au fournisseur (ou potentiellement accessibles aux autorités).

- **Transparence / audits** : les FAI ne publient pas forcément tous les audits de sécurité ni tous les détails de leur infrastructure, politiques de sécurité, etc.
- **Juridiction & obligations** : en France, les FAI peuvent être soumis à des obligations légales (accès aux données, demandes judiciaires etc.). Même avec le RGPD, il peut y avoir des cas de demandes légales ou d'inspection.
- **Fonctions avancées de sécurité** (chiffrement des métadonnées, sujet des mails, etc.) rarement prises en charge.
- **Discrétion** : les services spécialisés "privacy first" offrent souvent une meilleure discrétion, moins de collecte de métadonnées, etc.

Comparaison : FAI vs services spécialisés

Aspect	Avantages des serveurs des FAI français	Limites par rapport à services spécialisés
Proximité / juridiction nationale	Les données souvent hébergées en France ou au moins dans l'UE, donc sous lois françaises/européennes.	Mais cela ne garantit pas le niveau maximal de protection, surtout contre les autorités (lois de surveillance, demandes légales).
Disponibilité / support	Services fiables, support local, intégration avec d'autres services du FAI.	Parfois moins de fonctionnalités de confidentialité/discrétion.
Coût / simplicité	Inclus dans l'abonnement, facile à utiliser.	Services spécialisés peuvent coûter plus cher ou être moins "plug-and-play".
Confidentialité & chiffrement avancé	Généralement pas de chiffrement de bout en bout complet, moins de contrôle utilisateur sur les clefs, moins de protection des métadonnées.	Les fournisseurs privés axés sur la confidentialité excellent dans ces domaines.

Quelques exemples de services spécialisés

- **ProtonMail** : basé en Suisse, chiffrement de bout en bout, "zero-access" pour les mails chiffrés, audits, etc. SignalVault Privacy+2TechRadar+2
- **Tutanota (Tuta)** : très bon niveau de sécurité, cryptage y compris sujet / métadonnées dans certains cas, open source, etc. Wikipédia+1
- **Posteo** : basé en Allemagne, forte politique de confidentialité, anonymat possible, etc. Wikipédia+1
- **mail.fr** : "sécurisé", usage de protocoles de sécurité (SPF, DKIM, DMARC, DANE, DNSSEC), chiffrement du transport TLS, options pour chiffrement des emails entrants, etc. mail.fr

---

Classement proposé du plus faible au plus sûr

Voici un classement indicatif (subjectif, selon les informations publiques à ce jour) pour comparer les niveaux de sécurité/confidentialité d'adresses mails détenues sur différents types de serveurs :

Rang	Type de serveur / fournisseur	Ce qui le rend plus ou moins sûr
1 (le moins sûr)	Boîtes mails très basiques + FAI qui n'ont pas activé tous les protocoles, sans chiffrement fort, sans authentification multi-facteur. Ex : ancienne boîte "free.fr" ou "wanadoo.fr" si non mise à jour, ou un accès POP/IMAP non sécurisé.	Moins de chiffrement, possible interception, mots de passe faibles, métadonnées exposées ; moindre résistance aux demandes légales.

Rang	Type de serveur / fournisseur	Ce qui le rend plus ou moins sûr
2	FAI français “standard” actuellement : Orange, SFR, Bouygues, Free — avec les protections usuelles (TLS, mots de passe forts, authentification renforcée quand disponible), mais sans chiffrement de bout en bout, métadonnées accessibles, serveurs non audités publiquement.	Assez bon pour usage normal, mais “trusted third-party” (le fournisseur peut accéder aux données).
3	Services privés “sécurisés / respect de la vie privée” mais avec certaines limites : par exemple chiffrement partiel, ou lorsqu’on envoie à des correspondants non sécurisés, ou métadonnées encore visibles, ou juridiction moins forte. Exemples : mail.fr, Posteo, etc.	Meilleur contrôle, plus de transparence, mais encore dépendant dans certains cas des normes externes.
4	Services spécialisés premium / zero-access / end-to-end avec audits et forte protection des métadonnées, et où seul l’utilisateur contrôle les clés. Exemples : ProtonMail, Tutanota.	Meilleure confidentialité, très fortes protections, plus résistants à la surveillance ou aux failles internes.

Est-ce qu’on peut être *certain* que les serveurs des FAI français sont “bien protégés” ?

Non, on ne peut pas être “certain” dans l’absolu, parce que :

- Même les FAI très sérieux peuvent subir des failles, des incidents internes, des erreurs de configuration, ou être soumis à des demandes légales de remise de données.
- La protection dépend beaucoup de la façon dont l'utilisateur configure son compte (mot de passe, 2FA, accès via client tiers, etc.).
- Certains aspects comme la confidentialité des métadonnées (qui écrit à qui, quand, sujet, etc.) sont souvent moins bien protégés.

Est-il “mieux” de choisir un serveur non affilié à un FAI ?

Dans beaucoup de cas, **oui**, si ton objectif est la confidentialité / discrétion :

- Tu bénéficies souvent de meilleures garanties (end-to-end, anonymat, moins de métadonnées exposées).
- Tu peux choisir une juridiction avec des lois plus protectrices.
- Tu as plus de transparence dans certains cas (open source, audits, etc.).

Mais cela peut avoir des inconvénients :

- Coût plus élevé.
- Moins d’intégration / de support local.
- Potentiel de fiabilité moindre selon le fournisseur (sauf si c’est un fournisseur réputé).
- Certaines fonctions avancées ou compatibilité (clients mail, synchronisation, etc.) peuvent être moins simples.

Mon classement “moindre → meilleur” avec des exemples

Voici un classement plus concret avec quelques exemples pour illustrer :

Rang	Fournisseur ou type	Exemple / situations typiques
1	FAI français minimal, sans options de sécurité avancées	une boîte “@free.fr” ou “@wanadoo.fr” où le 2FA n’est pas activé, accès POP/IMAP non sécurisé ou avec mot de passe faible.
2	FAI français standard avec options de sécurité activées	ex. Orange, SFR, Bouygues, Free avec mot de passe robuste, avec ou sans 2FA, mais sans chiffrement de bout en bout.
3	Service privé “moyen-haut”	mail.fr, Posteo, etc. — de bons protocoles, bonne confidentialité, mais certaines limites selon les cas.
4	Service axé vie privée + chiffrement fort	ProtonMail, Tutanota, etc. — excellent choix si tu veux minimiser l’exposition, les métadonnées, etc.

Voici un classement sérieux + quelques recommandations précises, avec leurs avantages/inconvénients, afin de trouver le bon compromis sécurité à deux niveaux / budget ≦ 2-3 €/mois.

Recommandations de fournisseurs compatibles

Voici une liste de fournisseurs qui rentrent dans un budget modeste, avec ce qu’ils offrent, ce qui pourrait être limite, etc.

Fournisseur	Prix estimé / formule adaptée à ton budget	Ce qu’il offre de bon niveau de sécurité / confidentialité	Limites potentielles	Correspondance avec ton usage
Mailo (France)	L’offre *Premium* est à **1 €/mois** pour un compte, ~20 Go pour les mails + 5 Go pour le cloud. Mailo+3Mailo+3Mailo+3 Il y a aussi le pack *Family* pour 5 comptes Premium pour **2 €/mois**. Mailo+1	Serveurs en France, données hébergées en France, pas de publicité dans les offres payantes, bon support webmail / application, possibilité d’avoir alias, etc. → Sécurité de transport (TLS), bon niveau de service.	Pas nécessairement de chiffrement de bout en bout intégré pour tous les échanges, les métadonnées restent visibles, dépendant de la plateforme ; si tu veux forte confidentialité (PGP, etc.), il faudra probablement configurer cela toi-même.	Très bonne option : dans le budget, assez sûre, utilisable pour une asso, plusieurs comptes possibles via “Family”, utilisable depuis navigateur ou application.
Posteo (Allemagne)	~ **1 €/mois** pour une boîte mail standard avec ~2 Go (extensible) posteo.de+2posteo.de+2	Très bon niveau de confidentialité : open source, chiffrement des disques (LUKS), aucun suivi publicitaire, paiement anonyme possible, bon anti-spam, TLS / chiffrement en transit, bon respect de la vie privée. posteo.de+2posteo.de+2	Espace de stockage de base modeste (mais extensible), peut ne pas avoir toutes les options “cloud + apps” ou outils collaboratifs (agenda / drive) très poussés comme Infomaniak ou Mailo. Si beaucoup de pièces jointes ou stockage lourd, il faudra payer un peu plus.	Très bonne option si tu n’as pas besoin d’énormément de stockage et que le plus important est la confidentialité et simplicité.

Fournisseur	Prix estimé / formule adaptée à ton budget	Ce qu'il offre de bon niveau de sécurité / confidentialité	Limites potentielles	Correspondance avec ton usage
Tutanota	Offre "Premium (Private)" à ~ **1,20 €/mois** / utilisateur dans certaines formules, plus cher pour domaines multiples ou fonctionnalités d'équipe. Logiciels Pro	Chiffrement de bout en bout (plus complet que beaucoup d'autres), interfaces sécurisées, bonne réputation, open source, bon pour la vie privée.	Dans certaines formules, les comptes gratuits sont limités, certaines fonctionnalités avancées (alias, domaine personnalisé, ou intégration de client externe) peuvent ne pas être disponibles ou moins pratiques. Coût légèrement plus élevé que 1 €, selon ce que tu choisis.	Si tu veux niveau de confidentialité plus élevé, c'est une excellente option, mais peut dépasser légèrement ton budget selon les besoins (alias, stockage).
Infomaniak (Suisse)	Offre "Service Mail" dès **~1,50 €/mois** pour comptes avec domaine personnalisé / plusieurs adresses. assistance.email+1	Très bon niveau de sécurité et confidentialité : hébergement en Suisse, politique de respect des données, pas de pub, possibilité de chiffrer des mails via OpenPGP, bonne infrastructure, app mobile/web, bonne réputation.	Coût un peu plus élevé, pour obtenir plusieurs comptes ou beaucoup de stockage ça peut monter. Domaine personnalisé, alias, etc. sont souvent payants. Si tu es juste pour une boîte simple, c'est "sur le haut" de ton budget mais reste raisonnable.	Très sérieux choix si tu veux avoir le "plus" côté sécurité / confidentialité tout en restant dans une gamme raisonnable.
OVHcloud – "E-mail Pro"	**≈ 1,79 €/mois TTC / compte** pour "E-mail Pro" (France) avec 15 Go de stockage. OVHcloud	Serveurs en France, infrastructure mature, bon niveau TLS, outils FAI standards, réputation correcte, bonnes performances.	Moins d'options de confidentialité "extra" (chiffrement bout en bout, métadonnées, etc.) par défaut, moins centré "privacy first". Peut avoir des frais de domaine, etc.	Une option très raisonnable si tu veux rester dans un contexte français, bon rapport qualité/prix, mais moins "privé extrême".

Classement adapté (du "assez bon" au "meilleur", selon usage)

Voici comment je mettrais ces services dans un classement du plus "rapide à déployer mais sûre" au plus "privacité maximale", mais toujours adapté à des besoins réels

1. **Mailo** — excellent équilibre : prix très faible, plusieurs comptes possibles, stockage raisonnable, bonne sécurité, données en France → le plus "pratique + sûr" pour une association / usage courant.
2. **Infomaniak** — légèrement plus cher, mais très bonne réputation, avec options fortes de confidentialité, bon pour plusieurs comptes/domaine.
3. **Posteo** — très bonne confidentialité, faible coût, avec un peu moins de stockage ou quelques limitations, mais très solide pour protection des données.
4. **Tutanota** — pour aller plus loin dans la confidentialité (chiffrement, minimisation des métadonnées).

5. **OVHcloud E-mail Pro** — bon comme plan “sécurité standard / infrastructure française”, mais moins “privacy-first” dans les extras, donc placé ici pour ceux qui veulent rester dans un environnement français stable mais n’ont pas besoin du niveau maximal de discrétion.

Ce qui est recommandé

- **Option principale** : Utiliser **Mailo**, formule *Family* si vous avez 2-5 comptes, pour ~2 €/mois. Cela vous donne chaque utilisateur un compte Premium avec bon stockage, sans publicité, bonne expérience.
- En parallèle, si vous avez des mails particulièrement sensibles, on peut mettre en place du chiffrement, avec un client comme Thunderbird + PGP ou équivalent (affecte un peu la facilité, mais augmente la sécurité).
- Activer le **2FA** si le fournisseur le propose, utiliser des mots de passe robustes, vérifiez que les protocoles TLS sont bien utilisés, etc.
- Sauvegarde des mails ou export régulier, au cas où.
- **Option de secours** / “privacy upgrade” : Si Mailo semble insuffisant, passer à Posteo ou Tutanota pour les personnes qui veulent extra confidentialité.
