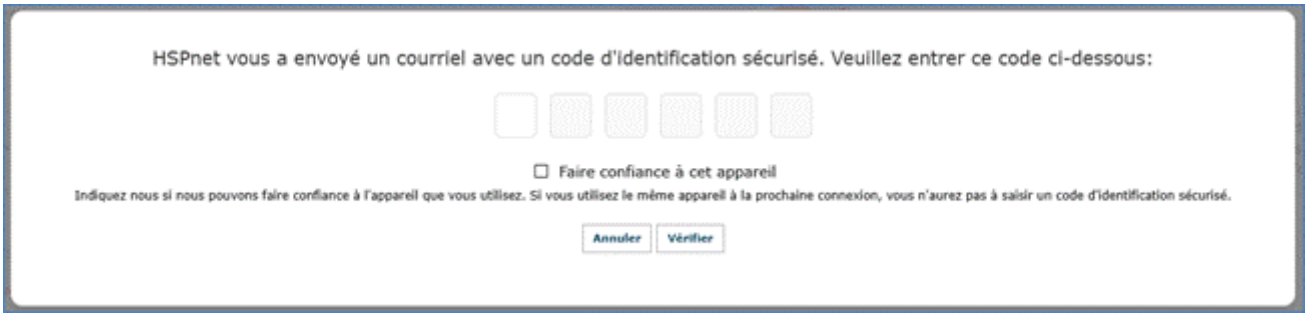
Authentification multifactorielle dans HSPnet

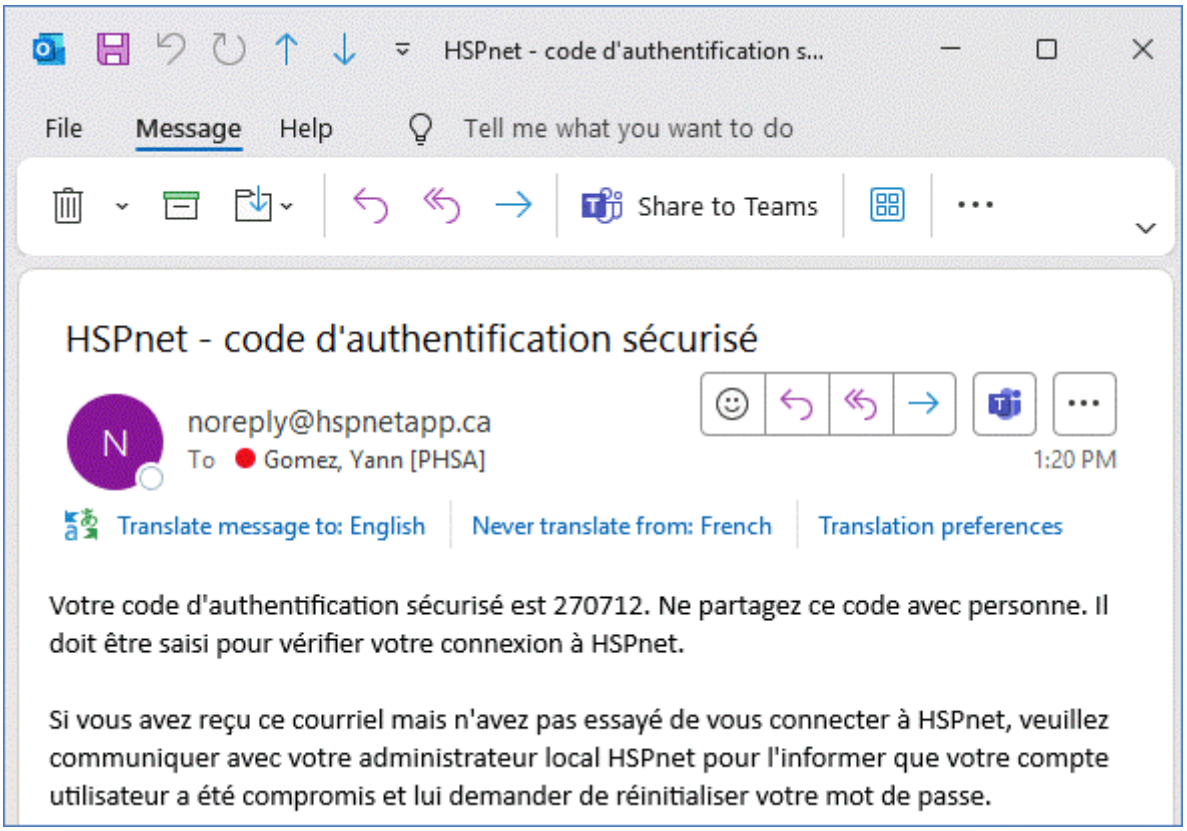
L'authentification multifactorielle (AMF) est une méthode de sécurité qui exige plusieurs moyens de vérification (facteurs) pour confirmer l'identité d'un utilisateur avant de lui permettre d'accéder à une application.

Dans HSPnet, cette exigence consiste en un code d'authentification envoyé par courriel. À chaque connexion, les utilisateurs doivent saisir leur code d’utilisateur et leur mot de passe, ainsi que ce code d'authentification. Les utilisateurs ont également la possibilité de sélectionner « Faire confiance à cet appareil » afin de pouvoir se connecter sur le même appareil sans saisir de code d'authentification.

Lorsque les utilisateurs sélectionnent l'option « Faire confiance à cet appareil », leur navigateur et son environnement sont enregistrés comme fiables, et ils n'ont plus besoin de code d'autorisation. L'accès depuis un autre navigateur ou appareil nécessiteun code d'authentification distinct pour se connecter.



Demande de code d’authentification AMF lors de connexion



Code d’authentification sécurisé

Rappelez-vous :

Les comptes d'utilisateur HSPnet sont autorisés et gérés par leur organisme.

- Chaque organisme est responsable de gérer ses utilisateurs, y compris l'attribution des rôles, la réinitialisation des codes d’utilisateur et mots de passe, ainsi que l'activation des comptes d’utilisateur
- Chaque organisme doit s'assurer que tous ses utilisateurs disposent d'une adresse courriel valide et fiable
  - Si un utilisateur utilise une adresse courriel partagée comme adresse principale, il doit fournir une deuxième adresse courriel personnelle et sécurisée (non partagée) pour recevoir le code d’authentification. Contactez l’assistance de HSPnet pour activer une 2^{e} adresse courriel
- Dans chaque organisme HSPnet, les administrateurs locaux peuvent mettre à jour les comptes d’utilisateur et les mots de passe associés. Si les utilisateurs ne parviennent pas à recevoir le code d'authentification par courriel, ils ne pourront pas se connecter à HSPnet. Les adresses courriel des utilisateurs peuvent être vérifiées et mises à jour si nécessaire à partir de l'écran « Maintenance du personnel ». Pour obtenir de l'aide à ce sujet, veuillez consulter les guides « Configuration de nouveaux comptes d'utilisateurs » et « Adresses courriel partagées » dans la base de connaissances.

À prendre en compte par les utilisateurs :

- L'utilisateur devra toujours saisir son nom d'utilisateur et son mot de passe. La procédure actuelle d'« Aide avec mot de passe oublié » reste inchangée
- Les utilisateurs auront la possibilité de cocher « Faire confiance à cet appareil » ; s'ils activent cette option, un cookie sera installé sur leur appareil et des informations relatives à leur environnement de navigation seront enregistrées
- Si un utilisateur choisit de ne PAS « Faire confiance à cet appareil », les informations relatives à son environnement de navigation ne seront pas enregistrées et aucun cookie ne sera installé. Il lui sera demandé de vérifier son identité à l'aide d'un code d'authentification lors de ses prochaines connexions
  - Si son navigateur est configuré en mode de navigation privée, les informations seront tout de même collectées et enregistrées lorsqu'il cochera « Faire confiance à cet appareil », mais le cookie ne sera pas conservé afin de considérer son appareil comme fiable
- Lors d'une connexion ultérieure, **si l'utilisateur commet une erreur sur son mot de passe ou si son environnement de navigation a changé**, son appareil ne sera plus considéré comme fiable, et un autre code d'authentification lui sera envoyé par courriel pour lui permettre de s'authentifier de nouveau
  - Si un gestionnaire de mots de passe est utilisé, **il doit être mis à jour lorsqu'un nouveau mot de passe est choisi dans HSPnet**. Sinon, l'ancien mot de passe non-valide sera inséré automatiquement à chaque connexion ce qui rendra l'appareil à ne plus être considéré fiable
- **Un utilisateur peut disposer de plusieurs appareils de confiance**. Chaque fois qu'il s'authentifie sur HSPnet à partir d'un nouvel appareil, il devra se faire vérifier à l'aide du code d'authentification. Une fois approuvé, chaque appareil sera mémorisé et il ne lui sera plus demandé de saisir à nouveau le code d'autorisation
  - Un appareil sera mémorisé pendant **une durée maximale de 30 jours**. Si des modifications apportées à l'appareil (ou à son environnement) sont détectées avant l'expiration de cette période de 30 jours, l'utilisateur sera invité à se faire vérifier à l'aide d'un code d'authentification

---

Révision #2
Créé 2026-07-24 14:55:27 UTC par Yann Gomez
Mis à jour 2026-07-24 15:18:24 UTC par Yann Gomez