MINISTÈRE
DE L'ÉDUCATION
NATIONALE

Liberté
Égalité
Fraternité

Mon authentification renforcée

Qu'est-ce que la double authentification ?

01-10-2026

ETNA
Environnement de Travail Numérique de l'Agent

Sommaire

Introduction 2
1. Qu'est-ce qu'un second facteur d'authentification (2FA) ? 2
2. Pourquoi le 2FA est-il indispensable ? 2
3. Comment fonctionne le 2FA ? 2
4. Les méthodes de 2FA les plus courantes 2
5. Bonnes pratiques pour utiliser le 2FA 3
6. Les limites et précautions à prendre 3
Conclusion 3

Introduction

Dans un monde où les cybermenaces sont de plus en plus sophistiquées, la protection des données et des comptes en ligne est devenue une priorité absolue. L'un des mécanismes les plus efficaces pour renforcer la sécurité est la **double authentification**, c'est-à-dire par l'usage d'un **second facteur** en plus du mot de passe. Cette protection supplémentaire permet de sécuriser l'accès aux services numériques, même lorsqu'un mot de passe a été compromis (hameçonnage, stealer). La double authentification constitue ainsi une **mesure essentielle pour protéger les comptes des agents et les données auxquelles ils accèdent**.
Ce tutoriel a pour objectif d'expliquer : 1. **Ce qu'est un second facteur d'authentification** 2. **Pourquoi il est essentiel** 3. **Comment il fonctionne** 4. **Les différentes méthodes disponibles** 5. **Les bonnes pratiques pour l'utiliser** 6. **Les limites et les précautions à prendre**

---

1. Qu'est-ce qu'un second facteur d'authentification (2FA) ?

L'authentification est le processus qui permet de vérifier l'identité d'un utilisateur avant de lui accorder l'accès à un système, un service ou une application. Traditionnellement, cette vérification repose sur un facteur unique, généralement un mot de passe. Cependant, les mots de passe peuvent être devinés, volés (par exemple via des attaques de phishing) ou compromis (en cas de fuite de données).
La double authentification combine deux moyens de vérification de l'identité de l'utilisateur : le mot de passe et un second facteur. Ce dernier est souvent abrégé en **2FA** et est appelé *Two-Factor Authentication* en anglais.*
Concrètement, après avoir saisi son identifiant et son mot de passe, l'utilisateur confirme son identité à l'aide d'un second facteur d'authentification.

---

2. Pourquoi le 2FA est-il indispensable ?

Le 2FA réduit considérablement les risques liés aux cyberattaques.
Voici pourquoi :

- **Protection contre le vol de mots de passe** : Même si un attaquant parvient à obtenir votre mot de passe, il ne pourra pas accéder à votre compte sans le second facteur.
- **Réduction des risques de fraude** : Les attaques par phishing ou par force brute deviennent bien moins efficaces.
- **Conformité aux réglementations** : De nombreuses institutions (banques, administrations, entreprises) sont tenues d'utiliser le 2FA pour se conformer aux normes en vigueur ou de sécurité, comme le **Règlement Général sur la Protection des Données (RGPD)**.

---

3. Comment fonctionne le 2FA ?

Le 2FA repose sur la combinaison de deux facteurs distincts, appartenant généralement à **trois catégories** :

1. **Quelque chose que vous connaissez** (ex. : un mot de passe, un code PIN)
2. **Quelque chose que vous possédez** (ex. : un téléphone, une carte à puce, une clé USB)
3. **Quelque chose qui vous appartient ou qui vous est propre** (ex. : une empreinte digitale, une reconnaissance faciale)

Exemple concret : Pour accéder à votre compte bancaire en ligne, vous devez :

1. Saisir votre mot de passe (facteur 1 : quelque chose que vous connaissez).
2. Valider un code envoyé par SMS ou généré par une application (facteur 2 : quelque chose que vous possédez).

---

4. Les méthodes de 2FA les plus courantes

Plusieurs technologies permettent de mettre en œuvre le 2FA :

- Envoi d'un code par SMS
- Génération d'un code par une application
- Utilisation d'une clé d'accès physique ou non
- Notification sur smartphone demandant une validation

Pour les agents des ministères, le choix a été fait de privilégier une solution reposant sur une application d'authentification qui présente deux avantages :

- une sécurité renforcée, grâce à la génération de codes temporaires à usage unique, sans dépendre de systèmes de messagerie ou de SMS ;
- le respect de la vie privée, puisque cette solution ne nécessite pas de communiquer son numéro de téléphone personnel ni aucune autre donnée à caractère personnel.

> La solution retenue par le ministère de l'Éducation nationale est le 2FA du type « codes temporaires à usage unique générés par une application mobile ». Ces codes sont appelés couramment « codes TOTP » (venant de l'anglais « Time-Based One-Time Password »). L'application d'authentification porte quant à elle souvent le nom « authenticator » et est installée sur le smartphone de l'agent (personnel si l'agent ne dispose pas d'un smartphone professionnel).

Si vous n'avez pas d'autre moyen d'authentification que par mot de passe et que vous n'avez pas de smartphone, vous devrez contacter l'Assistance académique pour bénéficier d'une solution alternative.

---

5. Bonnes pratiques pour utiliser le 2FA

Pour maximiser l'efficacité du 2FA, voici quelques recommandations :

1. **Privilégiez les applications d'authentification** plutôt que les codes SMS, plus vulnérables.
2. **Activez le 2FA sur tous vos comptes sensibles** (emails, banques, réseaux sociaux, outils professionnels).
3. **Ne partagez jamais vos codes 2FA** : Ils sont strictement personnels.
4. **Mettez à jour vos méthodes d'authentification** : Remplacez régulièrement vos clés ou applications si nécessaire.
5. **Utilisez dès que cela est possible un autre appareil que celui où vous vous authentifiez.**

---

6. Les limites et précautions à prendre

Bien que le 2FA améliore considérablement la sécurité, il n'est pas infaillible :

- **Attaques par phishing avancé** : Certains pirates utilisent des techniques pour intercepter les codes 2FA.
- **Perte ou vol du second facteur** : Si vous perdez votre téléphone ou votre clé de sécurité, l'accès à vos comptes peut être compromis voire temporairement perdu.
- **Complexité pour certains utilisateurs** : Le 2FA peut sembler contraignant, mais il est essentiel de s'y habituer pour une sécurité optimale.

Conclusion

Le second facteur d'authentification est un outil indispensable pour protéger vos données et vos comptes contre les cybermenaces. En combinant plusieurs facteurs d'authentification, vous rendez les attaques bien plus difficiles, voire impossibles, pour les pirates.
Pour résumer :

- **Activez le 2FA partout où c'est possible.**
- **Choisissez des méthodes sécurisées.** (applications ou clés physiques)
- **Sensibilisez votre entourage** à son importance.

En adoptant ces pratiques, vous contribuez à renforcer la sécurité numérique, tant pour vous-même que pour votre organisation.

Mon Aide Numérique

Tutoriels, FAQs et documentations

Version du document : 1

Dernière mise à jour le : 01-10-2026

https://monaidenumerique.education.gouv.fr