

La double authentification (MFA) expliquée simplement

Le réflexe qui bloque 99 % des piratages de comptes, même quand le mot de passe a fuité.

10 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/double-authentification

La double authentification (2FA ou MFA) ajoute une seconde preuve d'identité en plus du mot de passe : un code temporaire, une notification ou une clé physique. Même si votre mot de passe est volé, le compte reste protégé.

1. Comment ça marche

Après avoir saisi votre mot de passe (« ce que vous savez »), le service demande une seconde preuve : un code généré sur votre téléphone (« ce que vous possédez ») ou une empreinte (« ce que vous êtes »). Un attaquant qui a votre mot de passe ne peut pas franchir cette seconde barrière.

2. Quelle méthode choisir

- Application d'authentification (Google Authenticator, Microsoft Authenticator, Aegis...) : le meilleur rapport sécurité/simplicité
- Clé de sécurité physique (YubiKey...) : le plus haut niveau, recommandé pour les dirigeants et les administrateurs
- SMS : mieux que rien, mais vulnérable au détournement de carte SIM — à réserver en dernier recours

3. Où l'activer en priorité

- Messagerie professionnelle (c'est la clé de tous les autres comptes)
- Banque en ligne et outils de paiement
- Accès administrateur (serveurs, site web, nom de domaine, cloud)
- Outils métier contenant des données clients (CRM, facturation)
- VPN et accès distants

4. Les limites à connaître

La MFA n'est pas infaillible : les attaquants pratiquent la « fatigue MFA » (bombarder de notifications jusqu'à ce que la victime accepte par lassitude) et le phishing en temps réel, où un faux site relaie le code vers le vrai service. Les parades : refuser toute notification que vous n'avez pas déclenchée vous-même, et pour les comptes les plus sensibles, préférer les clés physiques FIDO2, insensibles par conception à ces deux attaques.

5. Déployer la MFA dans l'entreprise

Par où commencer

- Semaine 1 : messagerie et comptes administrateurs — le cœur du risque
- Semaine 2-3 : banque, outils de paiement, VPN et accès distants
- Ensuite : outils métier contenant des données clients (CRM, facturation, RH)
- Communiquer avant : expliquer le pourquoi en 5 minutes évite 90 % des résistances

Anticiper les cas particuliers

- Comptes partagés (réseaux sociaux, boîte contact) : centraliser le code dans le gestionnaire de mots de passe d'équipe, qui sait générer les codes TOTP
- Collaborateurs sans smartphone professionnel : clé physique ou génération du code sur le poste via le gestionnaire
- Prévoir la procédure « téléphone perdu » AVANT le premier incident : codes de secours stockés, second facteur de rechange, contact qui peut réinitialiser

CAS CONCRET

Cas fréquent en PME : la boîte email du dirigeant est compromise via un phishing pendant ses congés. Sans MFA, l'attaquant lit tout, se fait passer pour lui et déclenche un virement. Avec MFA, la connexion échoue, le dirigeant reçoit une notification inattendue — et l'attaque s'arrête là, transformée en simple alerte.

6. Et demain : les passkeys

Les passkeys (clés d'accès) remplacent progressivement le couple mot de passe + code : votre appareil s'authentifie par cryptographie, déverrouillée par votre empreinte ou votre visage. Ni mot de passe à voler, ni code à hameçonner — c'est le standard FIDO2 rendu grand public par Apple, Google et Microsoft. Activez-les dès que vos services les proposent : c'est à la fois plus sûr et plus rapide que tout ce qui précède.

L'essentiel à retenir

- 01 Activer la MFA sur la messagerie de tous les collaborateurs
- 02 Activer la MFA sur tous les comptes administrateurs
- 03 Privilégier une application d'authentification plutôt que le SMS
- 04 Conserver les codes de secours dans le gestionnaire de mots de passe
- 05 Définir la procédure « téléphone perdu » avant le premier incident
- 06 Refuser toute notification de connexion non sollicitée et la signaler
- 07 Adopter les passkeys sur les services qui les proposent

Questions fréquentes

Que se passe-t-il si je perds mon téléphone ?

C'est pour cela que chaque activation de MFA fournit des codes de secours : conservez-les dans le gestionnaire de mots de passe ou en lieu sûr. Avec eux, vous vous reconnectez et enregistrez un nouvel appareil en quelques minutes. Sans eux, il faut passer par la procédure de récupération du service — parfois longue. En entreprise, l'administrateur peut généralement réinitialiser le second facteur d'un collaborateur.

La MFA ne va-t-elle pas faire perdre du temps aux équipes ?

En pratique, la validation ne se produit que sur les nouvelles connexions (nouvel appareil, nouveau navigateur), pas à chaque ouverture de session : quelques secondes, quelques fois par mois. À comparer aux jours ou semaines perdus sur un seul compte piraté.

Le SMS est-il vraiment à éviter ?

Le SMS reste très supérieur à l'absence de MFA — activez-le si c'est la seule option. Mais il est vulnérable au détournement de carte SIM (un fraudeur se fait transférer votre numéro) et à l'interception. Dès qu'une application d'authentification ou une passkey est proposée, préférez-la.

Faut-il une clé physique (YubiKey) pour tout le monde ?

Non : l'application d'authentification suffit pour la plupart des usages. La clé physique se justifie pour les comptes à très fort enjeu — dirigeants, administrateurs systèmes, accès bancaires — car elle résiste au phishing en temps réel, ce que le code à 6 chiffres ne fait pas.

Pour aller plus loin

ANSSI — Recommandations sur l'authentification multifacteur — cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

Cybermalveillance.gouv.fr — la double authentification — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/double-authentification

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr