

## Comment activer l'authentification à deux facteurs?

L'activation de la 2FA varie d'une plateforme à l'autre, mais les étapes sont généralement assez similaires :

- 1. Accédez aux paramètres de sécurité** du compte que vous souhaitez sécuriser.
- 2. Recherchez** l'option permettant d'activer la **2FA** et sélectionnez-la.
- 3. Choisissez le deuxième facteur** que vous souhaitez utiliser (par exemple, SMS, application d'authentification, etc.).
- 4. Suivez les instructions** à l'écran pour configurer le deuxième facteur.
- 5. Testez** si tout est configuré correctement en vous déconnectant et en vous connectant à nouveau avec le deuxième facteur.



**Safeonweb.be**

## Par où commencer ?

- Commencez par votre compte mail
- Activez-la sur les sites web où vous laissez vos coordonnées bancaires : sites d'achats en ligne, sites de réservation de locations de vacances, site de réservation de tickets, site de revente, ...
- Protégez vos médias sociaux avec la 2FA

Bref, prenez l'habitude de l'utiliser partout où elle est disponible.

## Besoin d'aide ?

N'hésitez pas à demander de l'aide à votre famille ou des amis. Les collaborateurs des Espaces publics numériques (EPN) en Wallonie et Bruxelles sont également à votre disposition.



## Plus d'infos ?

Surfez sur [safeonweb.be](http://safeonweb.be)

# Suivez l'exemple de Herstappe : empêchez les cybercriminels d'entrer



Protégez vos comptes en ligne avec l'authentification à deux facteurs. Surfez rapidement sur [safeonweb.be](http://safeonweb.be)



**Safeonweb.be**

Si un pirate ou un escroc parvient à s'emparer de votre mot de passe, il peut :



utiliser votre boîte mail



jouer à votre place sur votre compte



passer des commandes en votre nom



publier quelque chose sur votre page Facebook, etc...

## Comment les escrocs peuvent-ils obtenir mes mots de passe ?

Utiliser des mots de passe forts est essentiel, mais les mots de passe seuls ne vous protègent pas suffisamment. Les escrocs volent ou devinent les mots de passe. Ou ils les obtiennent en usant d'une ruse (ils utilisent une excuse au téléphone ou vous convainquent de les saisir sur un faux site web). La probabilité que l'un de vos mots de passe soit visible sur Internet en ce moment même est assez élevée.

## Authentification quoi ?

La bonne nouvelle, c'est que vous pouvez éviter cela en utilisant une double clé en plus du mot de passe chaque fois que c'est possible : par exemple, la reconnaissance faciale ou l'empreinte digitale, un code envoyé sur votre téléphone portable. Un escroc peut s'emparer de votre mot de passe, mais il n'a aucune valeur sans la deuxième clé. C'est ce qu'on appelle l'authentification à deux facteurs ou 2FA. En fait, vous la connaissez déjà : ltsme est une forme de 2FA, si vous utilisez un digipass pour les services bancaires en ligne, il s'agit également d'une deuxième clé.



Safeonweb.be

Pour accéder à votre compte, vous devez prouver que vous êtes bien la personne que vous prétendez être.

Cela peut se faire de 3 manières ou avec 3 facteurs :

1. avec quelque chose que vous seul connaissez (votre mot de passe ou votre code PIN),



2. avec quelque chose que vous seul avez (votre téléphone via un code reçu par SMS ou une application d'authentification,



3. avec quelque chose que vous êtes (votre empreinte digitale, votre visage, votre iris...).



Généralement, vous utilisez l'un de ces facteurs, souvent un mot de passe, pour prouver qui vous êtes, mais il est préférable d'utiliser deux facteurs ou plus : on parle alors d'authentification à deux ou plusieurs facteurs (2FA ou MFA). Vous pouvez par exemple encoder un mot de passe et recevoir un code sur votre téléphone portable, ou utiliser votre empreinte digitale et une application pour accéder à votre compte.

## L'authentification à deux facteurs, c'est difficile ?

Vous ne savez pas comment activer l'authentification à deux facteurs sur vos comptes ? Les services les plus couramment utilisés offrent une forme d'authentification à deux facteurs et disposent d'une page de tutoriel assez courte.

Retrouvez les explications pour les principaux comptes sur [safeonweb.be/2FA](http://safeonweb.be/2FA).

Activez-la une fois pour ensuite ne plus y penser.



simple



rapide



extrêmement sûr