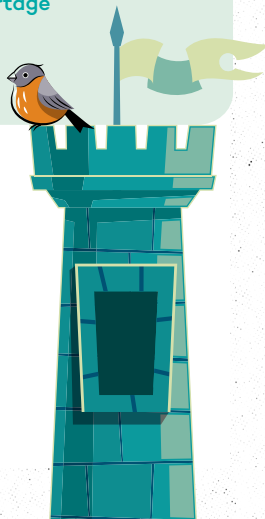


## Comment protéger vos comptes ?

1. Optez si possible pour une authentification à 2 facteurs (2FA).
2. Utilisez un gestionnaire de mots de passe.

### Nouveau dicton :

Un mot de passe, c'est comme un slip :  
on ne le laisse pas traîner, on ne le partage pas et on en change régulièrement !



**Protégez vos comptes  
en ligne avec  
l'authentification  
à deux facteurs.**

PLUS D'INFOS SUR  
**SAFEONWEB.BE**



**Les mots de passe,  
c'est dépassé.**



**Protégez vos comptes en ligne  
avec l'authentification à deux facteurs.**

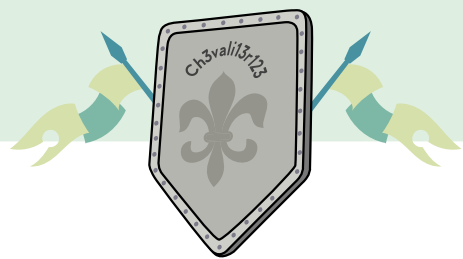
**Surfez sur safeonweb.be**

## Protégez doublement vos comptes en ligne avec l'authentification à 2 facteurs (2FA).

Facile et plus sûr.

Toutes les infos sur [safeonweb.be](https://safeonweb.be)

Les comptes en ligne (p. ex. : vos e-mails, les réseaux sociaux, les services bancaires en ligne et l'e-commerce) sont généralement protégés par un nom d'utilisateur et un mot de passe. Certains internautes choisissent des mots de passe faciles à retenir, et utilisent le même sur différents comptes. En agissant de la sorte, ils permettent aux hackers de pirater très facilement leur compte. Et si l'on posait les bons gestes pour éviter ce problème ?



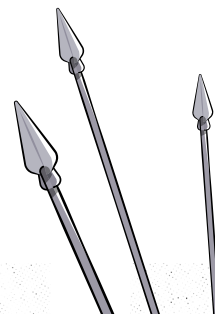
### 1. L'authentification à deux facteurs (2FA) : késako ?!

L'authentification à deux facteurs ou 2FA est une solution simple pour mieux protéger vos données.

Elle fonctionne comme une double écluse, ou comme un fossé et un pont-levis. Outre votre mot de passe, vous utilisez un code, qui est envoyé sur votre smartphone. Même si l'on vole votre mot de passe, vous disposez donc toujours d'une deuxième protection. Le hacker ne recevra pas ce code et ne pourra donc pas accéder à vos comptes !

#### ATTENTION !

Ne partagez **JAMAIS** vos identifiants avec des tiers. Certains escrocs vous demanderont parfois de fournir des codes de vérification par SMS, e-mail ou téléphone. Voilà une très mauvaise idée ! En coopérant, vous leur donnez carrément votre jeu de clés !



### 2. Trop de mots de passe à retenir ? Utilisez un gestionnaire de mots de passe.

Vous utilisez le même mot de passe sur chaque site ? Voilà qui est extrêmement risqué. Si votre mot de passe est subtilisé, le voleur peut utiliser votre mot de passe unique pour accéder à tous vos comptes qui ne sont pas protégés par l'authentification à 2 facteurs. Utilisez donc un mot de passe différent pour chaque compte. Un gestionnaire de mots de passe, c'est le meilleur allié pour retenir tous vos mots de passe. Ce coffre-fort virtuel assure la sécurité de tous vos comptes et mots de passe. Protégez bien ce coffre-fort par un mot de passe fort et si possible aussi par l'authentification à 2 facteurs. Vous n'aurez donc plus qu'un seul mot de passe à retenir. Une solution simple et plus sûre !

#### Gestionnaire de mots de passe

La plupart des gestionnaires de mots de passe peuvent en outre générer automatiquement des mots de passe uniques et sûrs. Vos mots de passe n'auront ainsi plus jamais rien à craindre.

**Protégez vos comptes en ligne grâce à l'authentification à 2 facteurs (2FA) combinée à un gestionnaire de mots de passe.**

PLUS D'INFOS SUR  
[SAFEONWEB.BE](https://safeonweb.be)

