



## Check-list Navigation sur les réseaux sociaux

Les réseaux sociaux offrent la possibilité d'interagir et d'échanger des informations. Cependant, les offres généralement gratuites ont un prix élevé : nos données personnelles. Voici 10 conseils pour naviguer en toute sécurité sur les réseaux sociaux.

1. Pour les profils sur les réseaux sociaux, la règle est toujours la même : divulguez peu de données personnelles !
2. Utilisez des mots de passe différents et sûrs pour les différents réseaux sociaux !
3. Vérifiez dans les paramètres de votre profil quelles données vous partagez et avec qui, et qui peut consulter votre profil.
4. Examinez les paramètres par défaut de la protection des données et limitez certains droits, par exemple la publicité personnalisée.
5. Choisissez comme photo de profil un espace réservé ou une photo neutre qui ne vous embarrassera pas plus tard.
6. Avant de télécharger un contenu sur Internet, réfléchissez si vous voulez le partager et avec qui. Souhaitez-vous qu'une image ou un rapport de statut reste sur Internet pour toujours ?
7. Remettez toujours en question les demandes de contact. L'expéditeur est-il authentique et digne de confiance ? Conseil : soyez particulièrement vigilant si quelqu'un se fait passer pour une connaissance ou un membre de la famille, et vous demande de l'argent ou des informations personnelles telles que votre numéro de téléphone portable.
8. Signalez les personnes qui vous harcèlent ou qui harcèlent d'autres personnes (« cyberharceleurs » et « trolls ») au réseau social concerné, par exemple si elles tentent de vous contacter sans y être invitées et de manière durable.
9. Documentez et signalez les textes, images, vidéos ou commentaires que vous considérez comme insultants et incitant à la haine, envers certains groupes de personnes. Par exemple ici : [meldestelle-respect.de](https://meldestelle-respect.de) et ici : [hateaid.org](https://hateaid.org).

10. Ne cliquez pas sur des liens au hasard. Les réseaux sociaux sont de plus en plus utilisés pour accéder à vos données personnelles et à vos comptes en ligne (hameçonnage).

## Comment reconnaître les fake news

Lorsque vous visualisez ou partagez des messages sur les réseaux sociaux, demandez-vous toujours : Est-ce que c'est vrai ?

- Qui est l'auteur du message ? Existe-t-il une source ?

**Conseil :** en cas de liens vers des portails d'information externes, il est utile de jeter un coup d'œil aux mentions légales du portail. Selon la législation allemande, les sites Internet en provenance d'Allemagne doivent comporter des mentions légales. Les mentions légales sont souvent mises en lien tout en bas d'un site Internet.

- Comment le message a-t-il été rédigé ? Des textes accrocheurs avec des images spectaculaires, associés à de nombreux points d'exclamation et d'interrogation, peuvent constituer un premier indice.
- Qui a rédigé le message ? Que sait-on de la personne ?
- D'autres sources sérieuses et des pages fiables de journaux ou d'émissions d'information ont-elles déjà rapporté les mêmes faits ?

**Conseil :** utilisez des fact-checkers. Vous pouvez vérifier sur [mimikama.org](https://mimikama.org), [tagesschau.de/faktenfinder](https://tagesschau.de/faktenfinder) ou [correctiv.org](https://correctiv.org) les fake news qui sont actuellement fortement diffusées.

- Où, quand et par qui une photo ou une vidéo a-t-elle été prise ? Que montre-t-elle vraiment ?

**Conseil :** la recherche inversée d'images de Google [images.google.de](https://images.google.de) ou de Bing permet de retracer l'origine d'une image et de savoir dans quel contexte elle a déjà été utilisée.

- Le message est-il actuel ? Y a-t-il une date et cette date peut-elle être exacte ?

**! Vous avez un doute ?** Demandez un conseil indépendant ! Vous pouvez obtenir des informations supplémentaires auprès de votre association de consommateurs (« Verbraucherzentrale »).  
[www.verbraucherzentrale.de](https://www.verbraucherzentrale.de)