Fiche Pratique N°86 : Vérifiez une information, une image ou une vidéo avant de la partager V1.1

15 nov, 2026 · @Gabriel

Objectif : *prendre trente secondes avant de partager pour reconnaître une fausse information, une image sortie de son contexte, une vidéo truquée ou une voix imitée par l'intelligence artificielle, en remontant vous-même aux sources, sans dépendre du verdict de qui que ce soit.*

- ***Public visé :*** *débutant*
- ***Temps estimé :*** *30 secondes pour les réflexes ; 5 minutes pour une vérification approfondie*
- ***Difficulté :*** ★☆☆☆☆ *(Très facile)*
- ***Prérequis :*** *un navigateur (Firefox conseillé, fiche N°2)*
- ***Fiches associées :*** *N°47 (arnaques en ligne), N°53 (utiliser l'IA sans livrer sa vie privée), N°85 (métadonnées des photos), N°67 (accompagner un proche débutant), N°17 (moteur de recherche), N°21 (flux RSS), N°76 (quitter Facebook et Instagram)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : le faux circule plus vite que le vrai

Une photo choquante, une citation indignée, une vidéo « que les médias vous cachent » : ces contenus sont faits pour être partagés vite, sous le coup de l'émotion. Certains sont des erreurs, d'autres des tromperies volontaires. Avec l'intelligence artificielle, fabriquer une fausse photo, une fausse vidéo ou une fausse voix est devenu facile et gratuit.

Situation	Conséquence
Vous partagez une photo d'inondation « d'hier »	C'était une photo d'un autre pays, prise il y a dix ans
Vous relayez une citation attribuée à une personnalité	Elle n'a jamais été prononcée
Vous regardez la vidéo d'un dirigeant qui annonce une mesure choc	C'est un hypertrucage (« deepfake ») fabriqué par IA
Votre « petit-fils » vous appelle, paniqué, pour un virement urgent	Sa voix a été clonée à partir de vidéos publiées sur les réseaux
Vous transférez une alerte « à faire suivre à tous vos contacts »	Vous participez sans le savoir à une rumeur ou à une arnaque

Une image pour comprendre : une information, c'est comme un colis. Avant de l'ouvrir, on regarde qui l'envoie, d'où il vient, et si l'emballage est intact. Une information sans expéditeur clair, sans date et qui vous presse de la faire suivre, c'est un colis suspect.

Le risque : propager une rumeur, nuire à quelqu'un, ou vous faire escroquer par une fausse voix.

Le bénéfice : des réflexes simples qui protègent votre portefeuille, votre réputation et vos proches.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°86 : Vérifiez une information, une image ou une vidéo avant de la partager V1.1

2. Comprendre les types de fausses informations

Type	Ce que c'est	Exemple
Désinformation	Information fausse, créée volontairement pour nuire	Une fausse annonce officielle
Mésinformation	Information fausse, partagée de bonne foi	Un proche qui relaie une rumeur en croyant aider
Malinformation	Information vraie, utilisée pour nuire	Une vraie photo privée diffusée pour humilier
Présentation partiale	Faits exacts, mais choisis ou cadrés pour orienter l'opinion	Un chiffre sorti de son contexte, que ce soit par un média, une entreprise, un parti ou une institution
Image hors contexte	Vraie photo, mais présentée avec une fausse date ou un faux lieu	Une photo de manifestation d'il y a dix ans présentée comme récente
Hypertrucage (deepfake)	Image, vidéo ou voix fabriquée par IA	Une vidéo d'une personnalité qui dit ce qu'elle n'a jamais dit

Avant de commencer

- ☐ J'accepte de **ne pas partager dans la minute** ce qui me met en colère ou m'émeut fortement
- ☐ J'utilise **Firefox** ou un autre navigateur à jour
- ☐ Je sais qu'**aucune source n'est infaillible** : je vérifie les faits, pas la réputation de celui qui parle
- ☐ J'ai convenu d'un **mot de passe familial** avec mes proches pour les appels urgents (section 4)

3. Pas à pas : les cinq réflexes en trente secondes

1. **Respirez.** Une information qui provoque une émotion forte (colère, peur, indignation) est faite pour être partagée sans réfléchir. C'est justement le moment de ralentir.
    - Vous devez voir : vous n'avez encore rien partagé.
2. **Qui parle ?** Cherchez la source d'origine : un média identifiable, un organisme officiel, une personne réelle. « Un ami d'un ami infirmier » n'est pas une source.
    - Vous devez voir : un nom, un site, une date. Sinon, méfiance.
3. **Quand et où ?** Vérifiez la date et le lieu. Beaucoup de fausses informations sont de vraies images d'un autre temps ou d'un autre pays.
    - Vous devez voir : une date et un lieu cohérents avec ce qui est raconté.
4. **Qui d'autre en parle, et d'où vient l'information ?** Tapez les mots-clés dans un moteur de recherche (fiche N°17). Croisez des sources indépendantes et de sensibilités différentes, et remontez à la **source d'origine** : le document, l'étude, le texte de loi, la vidéo complète.

gabriel.ananda@mailo.com
CC BY SA

   - Vous devez voir : la source d'origine elle-même, et non seulement des articles qui la résument ou la commentent.
5. **Dans le doute, ne partagez pas.** Ne pas partager ne fait de tort à personne.
   - Vous devez voir : un message non transféré, et la conscience tranquille.

Aucune source n'est infaillible, ni un réseau social, ni un média, ni un site de vérification, ni une institution. Tous peuvent se tromper, avoir une ligne éditoriale ou des intérêts. La bonne méthode ne consiste pas à choisir à qui faire confiance, mais à **vérifier les faits soi-même** : lire le document d'origine en entier, regarder qui finance qui parle, comparer des points de vue opposés, et distinguer les faits des commentaires.

4. Les arnaques à la voix clonée

Des escrocs imitent la voix d'un proche à partir d'extraits publiés sur les réseaux sociaux. Scénario typique : un appel d'un numéro inconnu ou masqué, une voix familière en détresse (« Maman, j'ai perdu mon téléphone et mon sac »), une demande d'argent ou de numéro de carte bancaire, en urgence.

1. **Convenez d'un mot de passe familial**, connu seulement de la famille. Évitez ce qui est public (nom de rue, nom de l'animal).
   - Vous devez voir : chaque membre de la famille connaît le mot et sait qu'il faut le demander en cas d'appel urgent.
2. **Raccrochez et rappelez** votre proche sur le numéro que vous connaissez, jamais sur celui qui vient d'appeler.
   - Vous devez voir : votre proche, joint à son numéro habituel, et en général tout étonné.
3. **Repérez les signes** : délais anormaux entre vos questions et les réponses, intonations bizarres, insistance sur l'urgence et le secret.
   - Vous devez voir : une conversation qui « accroche » ; ne donnez rien.

5. À quoi s'attendre et dépannage

Symptôme	Cause possible	Action
La recherche ne donne aucun autre article	Information inventée, ou très locale	Ne partagez pas ; attendez une confirmation
Une source la qualifie de fausse	L'information a peut-être déjà été démentie	Vérifiez les preuves avancées par cette source, puis répondez gentiment à celui qui vous l'a envoyée
La photo apparaît sur des sites anciens	Image sortie de son contexte	Notez la date d'origine trouvée par la recherche d'image
La vidéo semble étrange (lèvres décalées, mains bizarres, clignements absents)	Possible hypertrucage	Cherchez la vidéo sur le compte officiel de la personne

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°86 : Vérifiez une information, une image ou une vidéo avant de la partager V1.1

Symptôme	Cause possible	Action
Un proche insiste pour que vous partagiez	Pression sociale	« Je préfère vérifier avant » est une réponse respectable

À propos des sites de « vérification des faits » : beaucoup de médias et d'agences de presse en publient. Ce sont des médias comme les autres : ils ont une ligne éditoriale, des financements (certains ont été rémunérés par des plateformes comme Facebook pour ce travail) et peuvent se tromper ou être partiaux. Utilisez-les, si vous le souhaitez, comme une piste parmi d'autres : lisez leurs sources, pas seulement leur verdict.

Contenu illégal : une menace, un appel à la haine ou une escroquerie se signalent sur **Pharos**, la plateforme de signalement prévue par la loi.

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

6. Vérifier une image

1. **Recherche d'image inversée** : dans Firefox, clic droit sur l'image, puis copiez l'adresse de l'image ou enregistrez-la. Déposez-la dans un moteur de recherche d'images (TinEye, Bing Images, Google Lens).
    - Vous devez voir : les autres pages où l'image apparaît, et souvent sa date de première publication.
2. **Lisez ses métadonnées** si vous avez le fichier d'origine (fiche N°85) : date et appareil, parfois le lieu.
    - Vous devez voir : des informations cohérentes, ou rien du tout (fréquent après passage par un réseau social).
3. **Cherchez une signature d'origine (Content Credentials)** : déposez l'image sur `contentcredentials.org/verify`. Certains appareils et logiciels, y compris des générateurs d'images par IA, y inscrivent l'origine du fichier.
    - Vous devez voir : l'outil, l'appareil ou la mention « contenu généré par IA ». « No Content Credential » ne prouve rien : la plupart des images n'en ont pas, ou l'ont perdue.

7. Vérifier une vidéo

1. Installez le module **InVID-WeVerify** (gratuit, code libre, pour Firefox et Chrome), développé avec l'AFP et des chercheurs européens.
    - Vous devez voir : son icône dans la barre du navigateur.
2. Collez l'adresse de la vidéo dans l'outil **Keyframes** : il découpe la vidéo en images clés.
    - Vous devez voir : une série d'images fixes, à chercher ensuite par recherche inversée.
3. Utilisez la **loupe** pour examiner un détail (panneau, plaque, enseigne) qui indique le lieu.
    - Vous devez voir : un indice concret pour confirmer ou démentir le lieu annoncé.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°86 : Vérifiez une information, une image ou une vidéo avant de la partager V1.1

8. Les outils en un coup d'œil

Outil	Pour quoi	Points forts	Limites
Recherche d'image inversée (TinEye, Bing, Google Lens)	Retrouver l'origine d'une photo	Rapide, gratuit	Services non européens ; résultats variables
InVID-WeVerify	Vidéos et images	Gratuit, code libre (MIT), conçu pour les journalistes	Certaines fonctions passent par des services extérieurs
Content Credentials Verify	Origine d'un fichier, mention IA	Indique parfois explicitement un contenu généré par IA	La plupart des fichiers n'ont pas de signature
Sites de vérification des médias	Pistes et sources déjà rassemblées	Liens vers les documents d'origine	Ligne éditoriale et financements à connaître ; à lire comme une source parmi d'autres
Pharos	Signaler un contenu illégal	Plateforme officielle	Pas pour les simples erreurs

À propos des « détecteurs d'IA » : aucun n'est fiable à 100 %. Ils se trompent dans les deux sens. Le meilleur indice reste la source d'origine : qui a publié en premier, avec quelles preuves ?

À savoir avant de se lancer

Crainte fréquente	La réalité
« Je ne suis pas journaliste, je ne saurai pas vérifier. »	Les cinq réflexes de la section 3 suffisent dans la plupart des cas.
« Si c'est faux, quelqu'un l'aura déjà signalé. »	Le faux circule souvent plus vite que le démenti, et un démenti peut lui-même se tromper.
« Il suffit de croire les sources officielles. »	Une institution, un média ou une entreprise peut aussi présenter les faits de façon partiale. Vérifiez les documents eux-mêmes.
« Je reconnaîtrais la voix de mon fils entre mille. »	Les voix clonées sont devenues très convaincantes : le mot de passe familial est plus fiable que l'oreille.
« Ce n'est pas grave de partager, c'est aux autres de vérifier. »	Chaque partage donne du poids à l'information auprès de vos proches.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°86 : Vérifiez une information, une image ou une vidéo avant de la partager V1.1

Challenge 7 jours

- **Jour 1 :** appliquez les cinq réflexes à la première information choquante que vous recevez.
- **Jour 2 :** pour une information qui vous intéresse, remontez jusqu'au document d'origine (étude, texte de loi, vidéo complète) et lisez-le.
- **Jour 3 :** faites une recherche d'image inversée sur une photo virale.
- **Jour 4 :** convenez d'un mot de passe familial avec vos proches.
- **Jour 5 :** installez InVID-WeVerify et testez Keyframes sur une vidéo.
- **Jour 6 :** déposez une image sur `contentcredentials.org/verify` pour voir ce qu'il affiche.
- **Jour 7 :** expliquez l'arnaque à la voix clonée à un proche âgé.

Vous allez constater : quelques secondes de recul suffisent à déjouer la plupart des pièges.

En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Appliquer les cinq réflexes et remonter à la source	Un jugement indépendant, moins de rumeurs relayées	Section 3
Mot de passe familial	Protection contre la voix clonée	Section 4
Recherche d'image inversée	Les photos hors contexte démasquées	Section 6
InVID-WeVerify	Les vidéos vérifiées comme le font les journalistes	Section 7

À retenir absolument

- **Émotion forte = ralentir** avant de partager.
- **Qui, quand, où, d'où ça vient** : remontez à la source d'origine, quelle que soit la réputation de celui qui parle.
- **Appel urgent d'un proche : raccrochez et rappelez**, ou demandez le mot de passe familial.
- **Dans le doute, ne partagez pas.**

Test final :

1. Je connais les cinq réflexes avant de partager.
2. Je sais remonter jusqu'à la source d'origine d'une information.
3. Je sais faire une recherche d'image inversée.
4. Ma famille a un mot de passe pour les appels urgents.
5. Je sais où signaler un contenu illégal. ✅

Références

- Justice.fr – Signaler un contenu illégal publié sur Internet (Pharos)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°86 : Vérifiez une information, une image ou une vidéo avant de la partager V1.1

- InVID – InVID-WeVerify Verification Plugin
- Content Authenticity Initiative – Using the Verify tool
- Paris Match Belgique – Une arnaque imite la voix de vos proches (novembre 2025)

gabriel.ananda@mailo.com
CC BY SA