

Avant d'installer : la checklist sécurité d'un logiciel libre

Utilisez cette fiche pour évaluer rapidement un logiciel libre avant de le télécharger. Cochez chaque point : un doute important sur la source, la maintenance ou l'intégrité du fichier justifie de suspendre l'installation.

Au sommaire

1. Confirmer l'identité du projet
2. Choisir le canal de téléchargement le plus prudent
3. Vérifier que le projet est maintenu
4. Contrôler le fichier avant l'installation
5. Limiter les risques au moment d'installer

1. Confirmer l'identité du projet

☐

Identifier le nom exact du logiciel et son responsable

Fondation, entreprise, communauté ou développeur.

☐

Partir du site officiel du projet

Ne pas se fier uniquement à un résultat de recherche ou à un lien de forum.

☐

Recouper le site, le dépôt de code et la documentation

Les adresses, le nom de l'éditeur et la version doivent être cohérents.

☐

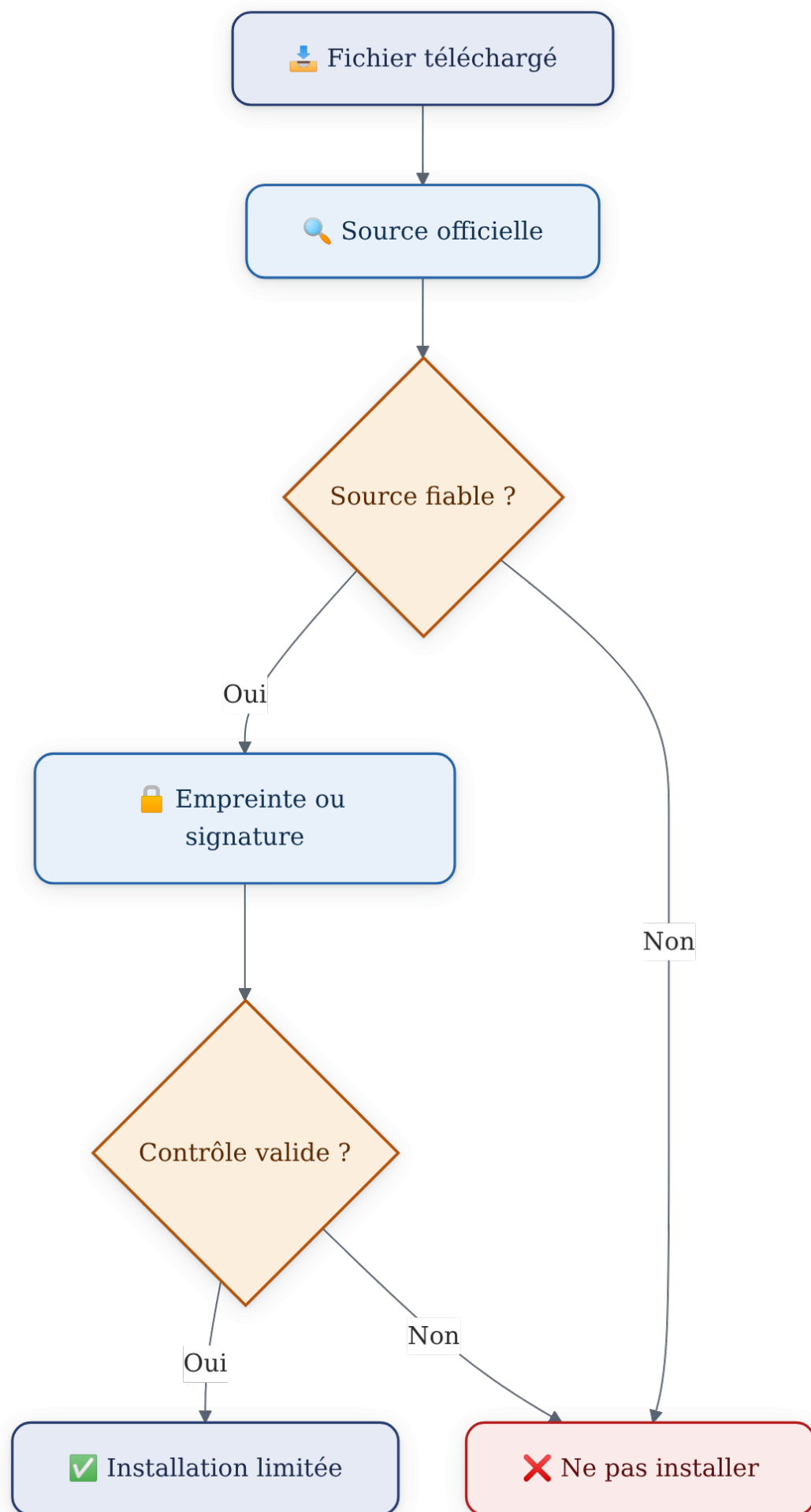
Vérifier la présence de notes de version et de documentation

Elles doivent correspondre au logiciel proposé.

☐

Repérer un canal de signalement des problèmes ou de sécurité

Un projet doit pouvoir recevoir et traiter les incidents.



SÉCURITÉ LOGICIELLE : CHOISIR LE BON CANAL D'INSTALLATION			
Chaque canal comporte des vérifications essentielles, des risques spécifiques et une décision recommandée.			
CANAL	CONTRÔLE À EFFECTUER	RISQUE PRINCIPAL	DÉCISION RECOMMANDÉE
Site officiel du projet	Adresse, version, empreinte et signature - Vérifier que l'adresse (URL) est exacte et utilise HTTPS. - Contrôler la version publiée. - Vérifier l'empreinte (hash) du fichier. - Vérifier la signature numérique du fichier ou de l'annonce.	Fausse copie ou lien détourné - Site miroir frauduleux. - Lien sponsorisé ou publicité menant à un site malveillant. - Contenu modifié ou tronqué. - Risque de vol de données ou d'installation de logiciels malveillants.	Comparer avec le dépôt officiel - Accéder au dépôt officiel du projet (code, annonces, téléchargements). - Comparer les informations : URL, version, empreinte, signature. - Ne faire confiance qu'en cas de correspondance exacte.
Dépôt officiel Linux	Nom du paquet et origine - Vérifier le nom exact du paquet. - Vérifier l'origine (dépôt officiel de la distribution). - S'assurer que le dépôt est signé par la distribution.	Paquet homonyme ou dépôt tiers - Paquet portant le même nom mais provenant d'une source non officielle. - Dépôt tiers non maintenu ou compromis. - Risque d'installer une version altérée ou instable.	Privilégier le dépôt de distribution - Utiliser en priorité les dépôts officiels de la distribution Linux. - N'ajouter un dépôt tiers qu'après vérification approfondie de sa légitimité et de sa fiabilité.
Boutique d'applications	Éditeur, version, permissions - Vérifier l'éditeur ou le développeur. - Contrôler la version proposée. - Examiner les permissions demandées par l'application. - Lire les avis et la politique de confidentialité.	Clone ou fonctions opaques - Application imitant une application légitime. - Permissions excessives ou injustifiées. - Fonctions opaques ou collectes de données cachées.	Recouper avec le site - Vérifier les informations sur le site officiel du projet. - Comparer l'éditeur, la version et les fonctionnalités. - En cas de doute, ne pas installer.
Site tiers	Recoupement solide requis - Rechercher des avis fiables et indépendants. - Vérifier l'authenticité du fichier (hash, signature si possible). - Confirmer la présence du logiciel sur le site officiel.	Installeur modifié - Installeur modifié ou injecté avec des logiciels indésirables. - Téléchargement piégé (bundles, malwares, adwares). - Absence de mises à jour et de support.	Éviter si source officielle non disponible - Éviter les sites tiers si le logiciel est disponible via un canal officiel. - En l'absence de source officielle, la prudence maximale s'impose. - Ne jamais exécuter un fichier d'origine douteuse.
RAPPEL CLÉ Toujours vérifier, toujours recouper, toujours privilégier la source officielle. Votre vigilance est votre meilleure protection.			

INFOGRAPHIE Comparatif des canaux de téléchargement pour renforcer la sécurité d'un logiciel libre.

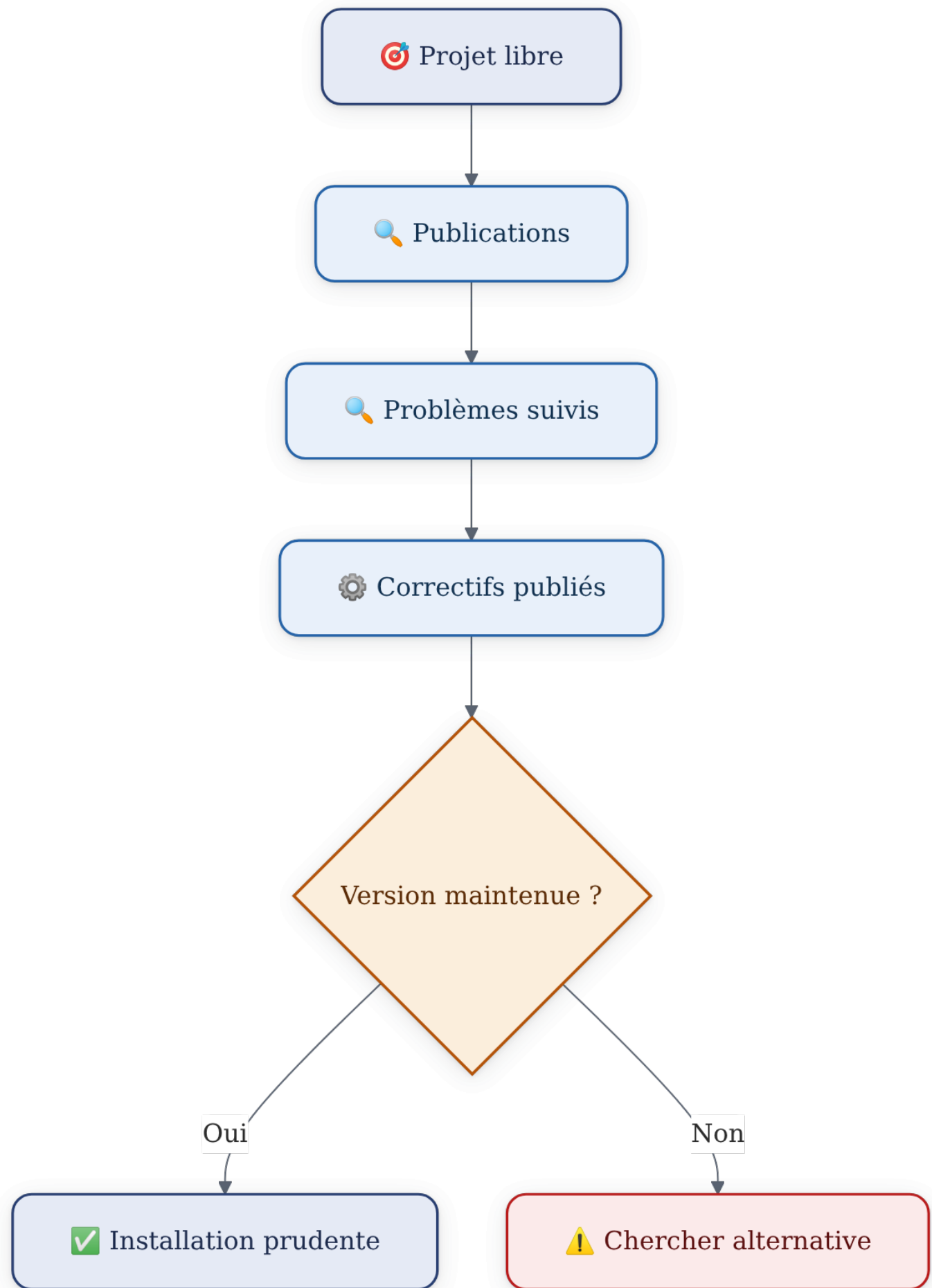
2. Choisir le canal de téléchargement le plus prudent

Canal	À contrôler	Décision prudente
Site officiel du projet	Adresse, version, empreinte et signature	Comparer avec le dépôt officiel
Dépôt officiel Linux	Nom du paquet et origine du dépôt	Privilégier les dépôts maintenus par la distribution
Boutique d'applications	Éditeur, version et permissions	Recouper avec le site du projet
Site de téléchargement tiers	Recoupement solide difficile	Éviter si une source officielle existe

3. Vérifier que le projet est maintenu

- ☐ **Noter la version exacte proposée au téléchargement**
- ☐ **Vérifier que cette version figure dans les publications officielles**
- ☐ **Consulter les notes de version et l'historique des publications**
Une publication identifiable indique que le cycle de mise à jour existe.
- ☐ **Rechercher les correctifs et les échanges sur les incidents**
Les réponses aux problèmes critiques comptent plus que la popularité.

-  **Examiner les problèmes ouverts liés aux crashes, aux accès non autorisés ou aux pertes de données**
-  **Écarter le logiciel si des incidents critiques restent sans réponse**
Surtout lorsqu'aucune version maintenue n'est annoncée.



4. Contrôler le fichier avant l'installation

- ☐ Télécharger le fichier depuis le canal officiellement désigné par le projet
- ☐ Comparer l'empreinte du fichier téléchargé avec celle publiée par le projet
Cela permet de vérifier que le programme correspond au fichier publié.
- ☐ Vérifier la signature numérique lorsqu'elle est fournie
- ☐ Suspendre l'installation si la version, l'empreinte ou la signature ne correspondent pas
- ☐ Éviter les installateurs republiés, les liens détournés et les plateformes inconnues
Particulièrement lorsqu'ils sont accompagnés de publicités agressives.

5. Limiter les risques au moment d'installer

- ☐ Lire les droits et permissions demandés par le logiciel
- ☐ Demander une justification claire pour tout droit administrateur
Un besoin non expliqué est un signal d'alerte.
- ☐ Identifier les dépendances lorsque le projet les publie
Une dépendance vulnérable ou abandonnée peut exposer un logiciel pourtant maintenu.
- ☐ Considérer les avis de sécurité publics et la liste des dépendances comme des signaux de transparence
- ☐ Isoler ou renoncer à installer un logiciel dont le niveau de maturité reste incertain

! Ne pas confondre licence et sécurité

Le code public, une licence open source, un grand nombre d'étoiles ou de téléchargements ne garantissent pas l'absence de faille. Le contrôle décisif porte sur la maintenance, les correctifs, les dépendances et la chaîne de téléchargement.

Cette checklist aide à réduire le risque avant installation ; elle ne remplace pas un audit de sécurité du code ou de l'environnement.