

Complément d'information

2025- 01- 15



L'actualité informatique
avec Denis Théorêt

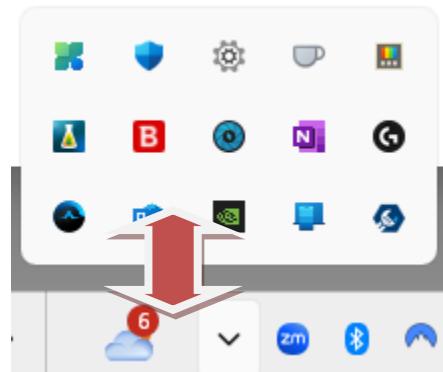
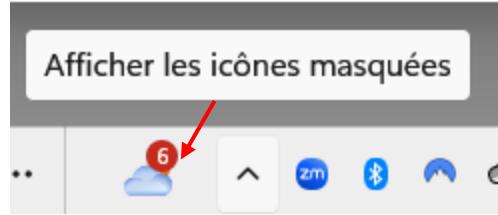
Pas de question

Trucs et astuces
avec Lucien Roy

Sylvie Veilleux fait remarquer à Lucien Roy que l'icône semble désactivée à l'écran!
Lucien Roy répond que c'est parce qu'ils sont dans les icônes cachées.

NDLR :

Comment "afficher les icônes cachées" sur la barre d'état Système, qui à droite de la "barre des tâches"



NDLR au sujet de PointerStick :

Site officiel : SoftwareOK.com

Lien pour télécharger :

[PointerStick 6.46 Pointeur virtuel sur votre bureau Windows](http://www.softwareok.com/pointerstick.htm)



(Captures d'écran, ne pas cliquer!)

Étape	Contenu
1. Qu'est-ce que PointerStick ?	<ul style="list-style-type: none"> - PointerStick est un petit logiciel gratuit (freeware) pour Windows. - Il affiche un « bâton pointeur » virtuel à l'écran, pratique pour les démonstrations, présentations, ou formations.
2. Principales fonctionnalités	<ul style="list-style-type: none"> - Permet d'ajuster la taille et la transparence du bâton pointeur. - Dispose de différents styles de bâtons ou couleurs. - Se lance facilement avec un clic, et peut rester en arrière-plan. - Consomme très peu de ressources.
3. Qui l'a développé ?	<ul style="list-style-type: none"> - Il est créé et maintenu par Nenad Hrg. - L'éditeur est le site SoftwareOK.com.
4. Source officielle et téléchargement	<ul style="list-style-type: none"> - Site officiel : SoftwareOK.com (rubrique “PointerStick”). - C'est la source de confiance pour obtenir la dernière version propre et sans ajout suspect. - On y trouve la version portable ou installable.
5. Installation et prise en main	<ol style="list-style-type: none"> 1. Rendez-vous sur le site officiel. 2. Téléchargez la version adaptée (32 bits, 64 bits, ou portable). 3. Ouvrez le fichier téléchargé pour lancer l'installation (ou utilisez la version portable). 4. Lancez PointerStick et ajustez les réglages (taille, style).
6. Conseils d'utilisation	<ul style="list-style-type: none"> - Testez plusieurs styles pour trouver celui qui vous convient. - Idéal à combiner avec un logiciel de capture d'écran ou un vidéoprojecteur. - Pour les formations ou présentations : gardez un accès rapide à PointerStick via la barre d'outils ou un raccourci.

En résumé : PointerStick est un outil pratique pour mettre en avant le curseur lors de présentations sous Windows. Vous pouvez le télécharger en toute sécurité sur le site SoftwareOK.com.

Marie-Claire Legault demande si c'est un utilitaire natif de Windows 11 et si elle est disponible avec Windows 10?

Lucien Roy répond que "Non", faut l télécharger à partir de leur site seulement:
Convient pour : Windows 11, Windows 10, 8.1, 7,

Cybermenaces 2025 vs Aînés

Avec Michel Cloutier

Louise Dubreuil parle de la chronique de François Charron parue le 6 janvier 2025 où on parlait que Chrome/Edge était transformé en virus dans le temps des fêtes?
André Carrier a mis le lien dans le clavardage :



(Capture d'écran, ne pas cliquer!)

Lien direct :

[**32 extensions Chrome transformées en virus pour voler nos données**](#)

Louise Dubreuil demande ce qu'est une extension*

Lucien Roy répond que c'est un ajout ou une fonction à un navigateur

Louise Dubreuil veut savoir comment être certain qu'il n'y a pas de virus

Sylvie Veilleux n'est pas d'accord et mentionne qu'il faut toujours se méfier

Sylvie Veilleux ajoute qu'une extension est un outil qu'on ajoute au navigateur **Lucien Roy** recommande afin d'éviter des problèmes de mettre à jour les navigateurs que vous utilisez, surtout ceux que vous n'utilisez pas souvent.

NDLR au sujet des extensions en collaboration de l'IA ChatGPT :

Extensions pour Navigateurs Edge et Chrome

Aspect	Détails	Exemples d'extensions	Liens vidéo
Qu'est-ce qu'une extension?	Une extension est un petit programme qui modifie ou améliore l'expérience de navigation en ajoutant des fonctionnalités au navigateur.	- Adblock Plus : bloque les publicités. - Grammarly : aide à corriger la grammaire et l'orthographe. - LastPass : gestionnaire de mots de passe.	Qu'est-ce qu'une extension ?
Pourquoi utiliser des extensions?	Pour personnaliser et optimiser la navigation, améliorer la productivité, ou ajouter des outils de sécurité.	- Google Translate : traduction rapide de pages. - Pocket : enregistrer des pages pour plus tard.	Pourquoi installer des extensions ?

		<ul style="list-style-type: none"> - HTTPS Everywhere : forcer la connexion sécurisée. 	
Comment installer une extension ?	<ol style="list-style-type: none"> 1. Ouvrir le magasin d'extensions du navigateur (Chrome Web Store ou Microsoft Edge Add-ons). 2. Rechercher l'extension souhaitée. 3. Cliquer sur « Ajouter » et suivre les instructions. 	<ul style="list-style-type: none"> - Bitdefender Anti-Tracker (protéger la vie privée). - Loom : pour enregistrer des vidéos directement dans le navigateur. 	Installation d'extensions sur Chrome
Gestion des extensions	Les extensions peuvent être activées, désactivées ou supprimées depuis le menu des extensions dans les paramètres du navigateur.	<ul style="list-style-type: none"> - Evernote Web Clipper : capturer et sauvegarder des pages web. - Trello : gestion de projet via le navigateur. 	Gérer les extensions
Sécurité et extensions	Certaines extensions peuvent être malveillantes. Il est important de vérifier les avis et les permissions demandées avant d'installer.	<ul style="list-style-type: none"> - Privacy Badger : bloque les trackers. - NoScript : contrôle des scripts JavaScript. 	Sécurité des extensions

Exemples Concrets d'Utilisation

1. Navigation Plus Fluide : Utiliser Adblock Plus pour éviter les publicités intrusives et gagner du temps en ligne.
2. Sécuriser votre Connexion : Installer HTTPS Everywhere pour vous assurer que toutes les connexions à des sites web utilisent une sécurité maximale (HTTPS).
3. Optimisation de la Productivité : Utiliser Pocket pour enregistrer des articles intéressants à lire plus tard, sans être distrait pendant la navigation.

Vidéos en Français/Québécois

1. [Comment installer une extension sur Chrome](#)
2. [Sécuriser votre navigation avec des extensions](#)
3. [Extensions Chrome pour la productivité](#)

Cybersécurité et Extensions de Navigateur

Risques liés aux Extensions

Les extensions de navigateur, bien qu'utiles, peuvent constituer un vecteur de cybermenaces si elles ne sont pas installées avec soin. Voici les principaux risques associés :

1. **Collecte de Données Personnelles** : Certaines extensions peuvent avoir accès à votre historique de navigation, à vos mots de passe, ou même à vos informations sensibles.
2. **Malware (logiciels malveillants)** : Certaines extensions peuvent contenir des logiciels malveillants, comme des **trojans**, qui peuvent espionner vos activités ou infecter votre appareil.

3. **Phishing et Escroqueries** : Des extensions malveillantes peuvent être utilisées pour rediriger les utilisateurs vers des sites de phishing ou voler leurs informations de connexion.
4. **Exploitation des Permissions** : Même si les extensions sont approuvées par les stores (Google Store ou Microsoft Store), elles peuvent demander des permissions excessives pour récolter plus de données qu'elles ne le devraient.

Chronique de François Charron – 6 janvier 2025

Dans sa chronique, François Charron aborde probablement les risques croissants associés à l'utilisation des extensions de navigateur, notamment les **extensions frauduleuses** ou malveillantes qui contournent les mesures de sécurité des stores. En effet, même avec des vérifications, des extensions dangereuses peuvent passer entre les mailles du filet.

Charron aurait probablement mis en garde contre ces risques en expliquant que, même en téléchargeant depuis des sources réputées, il existe toujours un **risque résiduel**.

Les Stores Officiels : Plus Sûrs mais Pas Infaillibles

Les **Microsoft Store** et **Google Chrome Web Store** ont des systèmes de vérification en place pour filtrer les extensions malveillantes.

Cependant, ces systèmes ne sont pas parfaits et peuvent laisser passer des extensions nuisibles. En voici les points clés :

- **Google Chrome Web Store** : Google effectue des vérifications de sécurité sur les extensions, mais certains développeurs trouvent des moyens de contourner ces contrôles.
Les extensions doivent être constamment surveillées, et les utilisateurs doivent toujours vérifier les permissions demandées.

- **Microsoft Store** : Microsoft effectue également une vérification des applications et extensions avant leur publication. Cependant, tout comme Google, des extensions malveillantes peuvent parfois échapper à la vigilance, notamment si les mises à jour contiennent des modifications malveillantes.

Conseils pour Minimiser les Risques

Même en téléchargeant des extensions à partir des **stores officiels**, il est essentiel de rester vigilant :

1. **Vérifier les Avis et Évaluations** : Toujours lire les critiques et les évaluations d'une extension avant de l'installer.
Les avis négatifs ou un grand nombre de plaintes peuvent être des indicateurs d'extensions problématiques.
2. **Vérifier les Permissions Demandées** : Ne jamais ignorer les permissions demandées par l'extension.
Si une extension demande des accès qui semblent excessifs ou inutiles pour sa fonctionnalité (par exemple, l'accès à vos mots de passe ou à votre historique de navigation), c'est un signal d'alarme.
3. **Mettre à Jour les Extensions** : Toujours garder ses extensions à jour. Les mises à jour peuvent corriger des vulnérabilités et des failles de sécurité.
4. **Utiliser un Antivirus ou un Outil de Sécurité** : Certains antivirus et outils de sécurité offrent une protection supplémentaire contre les extensions malveillantes.
5. **Prudence avec les Extensions Populaires** : Les extensions populaires ont souvent plus de visibilité et sont donc plus souvent ciblées par les cybercriminels.
Par conséquent, il est important de suivre des sources sûres et de n'installer que celles dont on a réellement besoin.

Conclusion

En résumé, même si télécharger des extensions depuis les **Microsoft Store** ou le **Google Web Store** réduit les risques, cela ne les élimine pas complètement. La vigilance reste de mise.

François Charron a certainement mis en lumière l'importance de vérifier les extensions avant de les installer, de faire attention aux permissions et d'installer des outils de sécurité pour éviter les pièges.

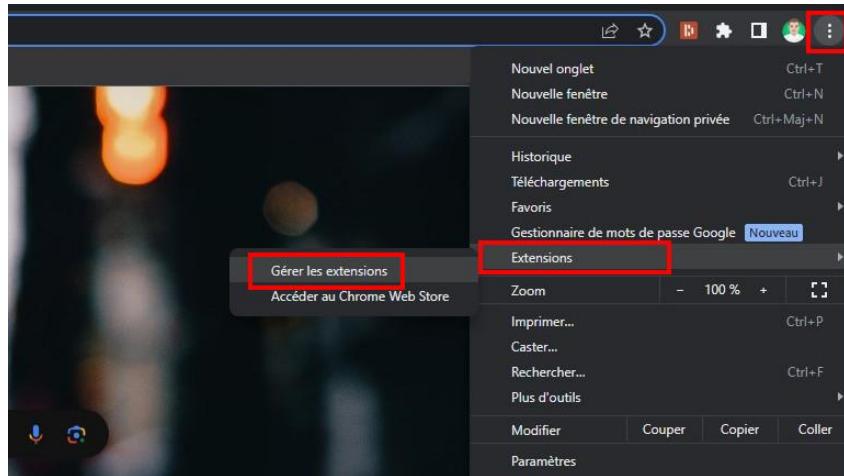
Suppléments d'Information

- Comment supprimer les extensions malveillantes sur nos navigateurs
 - Lien proposé par François Charron :
[Comment supprimer les extensions malveillantes sur nos navigateurs](#)
- Comment donc voir si une extension malveillante se cache sur notre navigateur?
Voici la marche à suivre pour faire un petit coup de ménage sur la majorité des navigateurs sur le marché.
 - [Supprimer une extension sur Google Chrome](#)
 - [Supprimer une extension sur Brave](#)
 - [Supprimer une extension sur Mozilla Firefox](#)
 - [Supprimer une extension sur Microsoft Edge](#)
 - [Supprimer une extension sur Safari d'Apple](#)
 - [Supprimer une extension sur Opera](#)

Exemple : Comment supprimer une extension sur Google Chrome

Google Chrome est le navigateur internet pour ordinateur le plus populaire au monde. Heureusement, il est très simple d'y gérer nos extensions. Pour ce faire, il faut suivre ces étapes:

- Ouvrir **Chrome**
- Cliquer sur les **trois petits points verticaux** dans le coin supérieur droit
- Placer sur son curseur sur l'onglet: **Extensions**
- Cliquer sur l'option: **Gérer les extensions**



Voici où aller sur le navigateur Google Chrome pour ordinateur afin de gérer les extensions

On doit ensuite regarder la liste et les icônes des extensions, identifier celles que l'on n'utilise pas et appuyer sur l'option: Supprimer.

Si notre ordinateur continue toujours à agir bizarrement après la suppression de l'extension qu'on jugeait étrange, alors il est préférable de faire un scan avec un **bon antivirus**.

Période de questions, suggestions et commentaires



(Image créée par Dream Lab l'IA de Canva.com)

Marc Severe mentionne que si on ajoute la fonction Traductor, il est possible de lire un journal dans la langue choisie.

Lucien Jutras utilise un ordinateur Mac (Apple) qui date de 2013; n'a plus de support d'Apple, sa dernière mise à jour de macOS 10.15.

Il y a une importante mise à jour, avec le navigateur Google, mais il reçoit un avis que la version 128.x du navigateur de Google sera la dernière.

Sylvie Veilleux mentionne que c'est son système d'exploitation qui n'est pas à jour.

NDLR et selon l'analyse de ChatGPT, faudrait impérativement que Monsieur Jutras télécharge la mise à jour macOS 10.16 pour accéder aux dernières mises à jour de Google. Il en va de la sécurité de ses activités de navigation...

On parle de code, pour sécuriser ses accès aux sites :

Sylvie Veilleux parle de la double identification. Exemple : Cyberimpact (messagerie qu'on utilise pour les mémos-infos)

On nous envoie un code à une certaine adresse courriel; on copie et on colle le code et ainsi on a accès à Cyberimpact.

Marc Severe dit que pour ouvrir Facebook avec le navigateur Chrome, ça va, mais s'il change de navigateur il a des problèmes.

Michel Cloutier mentionne fait un test avec Chrome et on lui propose un CAPTCHA (acronyme de l'anglais "Completely Automated Public Turing test to tell Computers and Humans Apart") est une mesure de sécurité de type "authentification par question-réponse".

Sylvie Veilleux ajoute que si vous ne vous déconnectez pas de Facebook, en l'ouvrant de nouveau ça va aller

Marc Severe dit que c'est lorsqu'il est en voyage qu'il n'y arrive pas, mais pas quand il est ici.

Michel Cloutier suggère à **Marc Severe** de se déconnecter et de se connecter de nouveau, ainsi il devra inscrire ses identifiants à nouveau.

Marie-Claire Legault suggère à **Marc Severe** de nous en donner des nouvelles la semaine prochaine.

Gérard Baudry dit qu'il a environ 3000 courriels dans la corbeille et demande si cela peut ralentir?

Marie-Claire Legault ajoute que les courriels envoyés prennent aussi beaucoup de place et suggère de faire le ménage.

NDLR avec l'analyse de l'IA de Microsoft Copilot :

Voici d'abord un tableau des conséquences de conserver autant de courriels inactifs:

Conséquence	Détails
Stockage	Accumuler un grand nombre de courriels, surtout avec des pièces jointes, utilise beaucoup d'espace de stockage, pouvant entraîner des frais supplémentaires.
Performance	Un grand volume de courriels peut ralentir la performance de l'application de messagerie, rendant l'accès et la recherche des messages plus lentes.
Sécurité	Les courriels anciens peuvent contenir des informations sensibles qui, si non sécurisées, pourraient être vulnérables aux failles de sécurité.
Gestion difficile	La recherche de courriels spécifiques devient difficile et chronophage avec un grand volume de courriels accumulés.
Déduplication	Peut contenir des courriels en double ou obsolètes, rendant l'organisation et la gestion des courriels plus compliquée

Pour la deuxième mission, voici un tableau simple sur l'organisation qu'il devra s'engager rigoureusement:

Étape	Actions
1. Tri initial	Parcourir les courriels et supprimer ceux qui ne sont plus nécessaires, comme les anciens messages promotionnels, les spams et les courriels non pertinents.
2. Catégorisation	Créer des dossiers ou des étiquettes pour organiser les courriels restants en catégories telles que "Travail", "Personnel", "Projets", etc.
3. Archivage	Archiver les courriels importants mais non urgents pour les garder hors de la boîte de réception tout en les conservant accessibles si besoin.
4. Gestion continue	Établir une routine hebdomadaire ou mensuelle pour trier et organiser les nouveaux courriels afin de ne pas laisser l'accumulation se reproduire.
5. Sauvegarde	Sauvegarder régulièrement les courriels importants sur un support externe ou un service cloud sécurisé pour éviter toute perte de données.

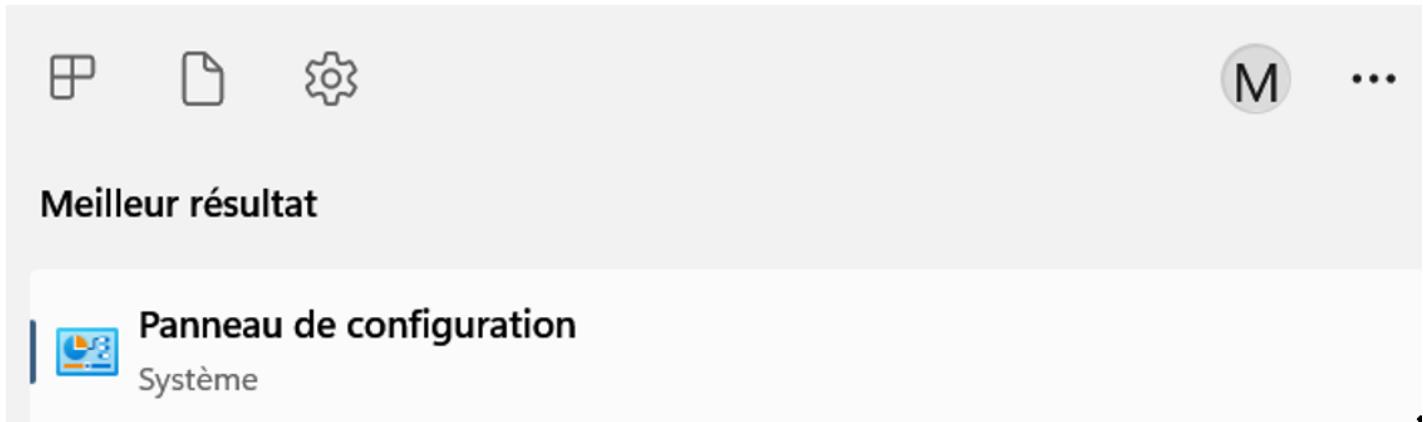
Jacques Paquet demande comment faire pour désinstaller l'antivirus McAfee de son PC, qui s'est introduit ?

NDLR et suivre les étapes suivantes :

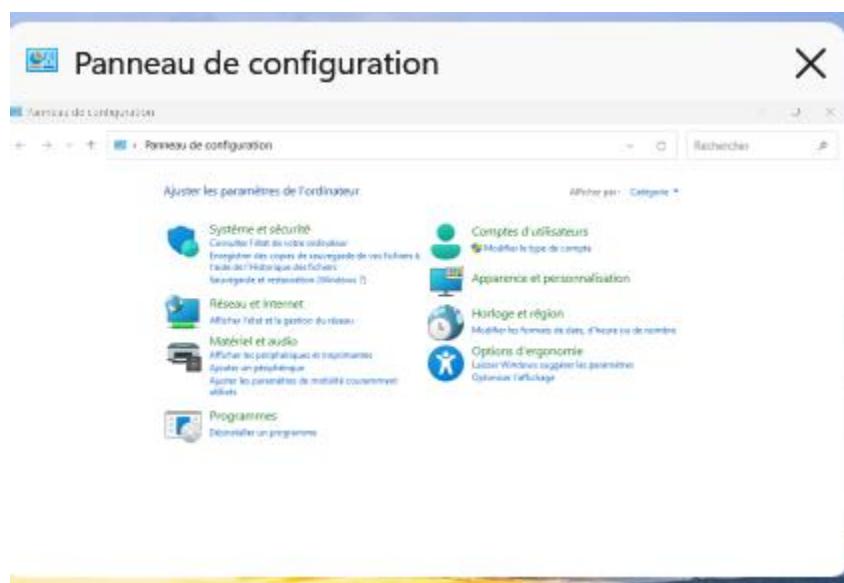
1. Coin inférieur gauche à la droite du menu "démarrer" :
 - a. Cliquer sur la "loupe" ou bouton de recherche



- b. Taper dans la barre de recherche : "panneau de configuration"
- c. Cliquer sur l'icône



- d. Une fois la boîte de dialogue ouverte



- e. Trouver et cliquer sur "Programmes" et Désinstaller un programme



f. Le panneau d configuration > Programmes > Programmes et fonctionnalités

Nom	Éditeur	Installé le	Taille	Version
4K Tokkit	Open Media LLC	2025-01-03	402 Mo	2.7.4.960
ActMask Universe Virtual Printer SDK		2024-07-13	1,14 Mo	
Antidote - Connectix 12	Druide informatique inc.	2024-12-23	475 Mo	12.1.1307
Antidote 12	Druide informatique inc.	2024-12-23	289 Mo	12.1.1307
Antidote 12 - English module	Druide informatique inc.	2024-12-23	919 Mo	12.1.1307
Antidote 12 - Module français	Druide informatique inc.	2024-12-23	905 Mo	12.1.1307
Ashampoo App	Ashampoo GmbH & Co. KG	2024-08-20		2.1.1
Ashampoo Backup Pro 26	Ashampoo GmbH & Co. KG	2024-11-19		26.00
Ashampoo Driver Updater	Ashampoo GmbH & Co. KG	2024-07-26		1.6.2

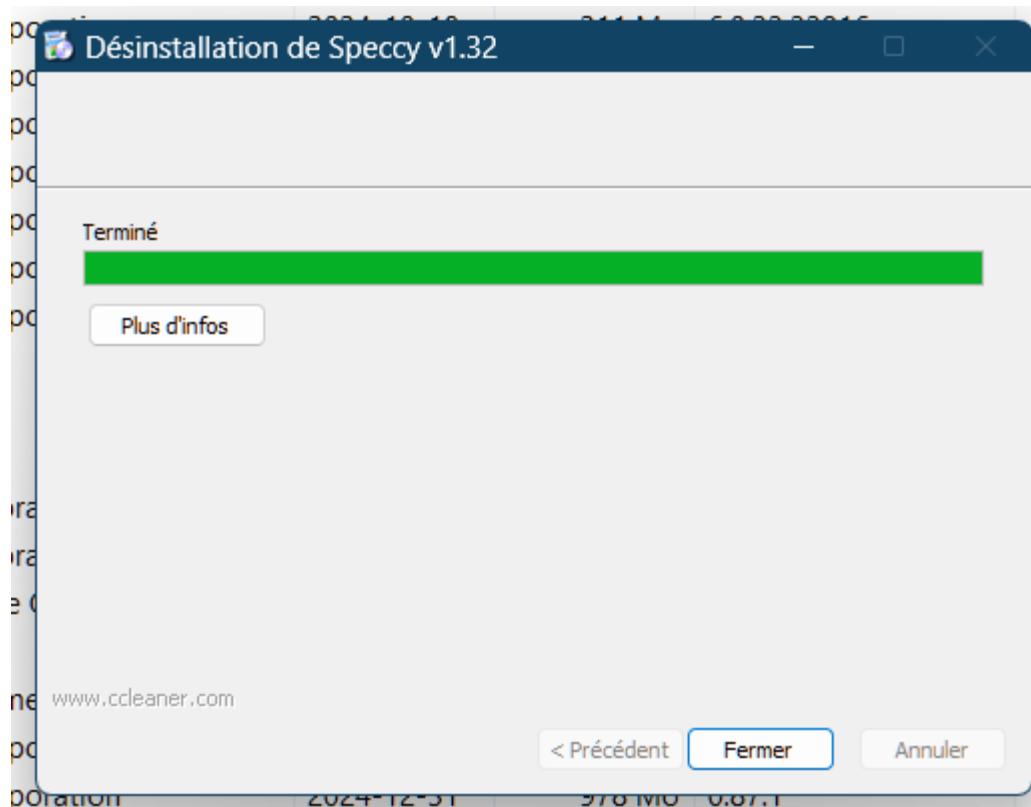
g. Sélectionner le ou les programmes “fautifs”

h. Pointer sur le programme fautif avec la souris avec le bouton gauche ou que vous désirez désinstaller

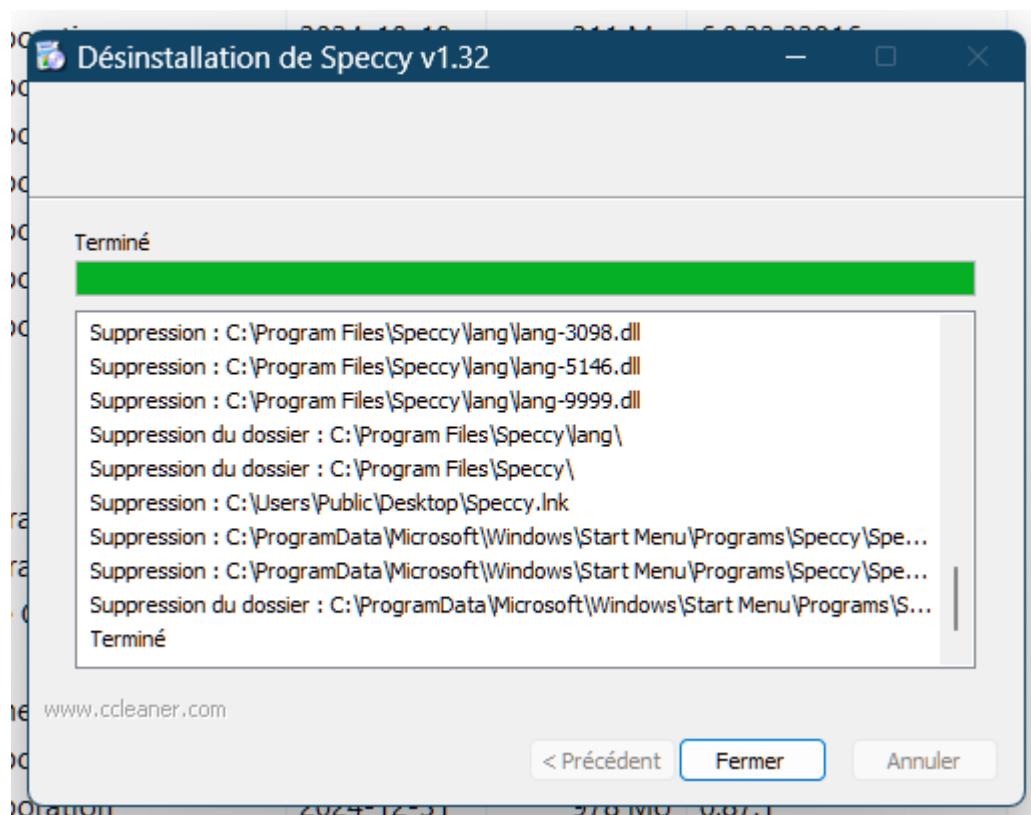
i. Cliquer sur “Désinstaller/Modifier”

Samsung USB Driver for Mobile Phones	Samsung Electronics Co., Ltd.	2024-10-18	41,5 Mo	1.7.58.0
Speccy	Piriform	2024-10-18		1.32
Stellar Di	Désinstaller/Modifier			

j. Une boite de dialogue s'ouvre qui montre la barre de désinstallation



k. Attendre que le bouton “Terminer” ou Fermer, soit apparent



- I. Fermer toutes les opérations dans le même ordre et pour s'assurer que le ou les programmes non-désirés sont bel et bien désinstallés...
- m. Redémarrer votre ordi et accéder le panneau de configuration pour s'assurer que la désinstallation s'est bien déroulée



(Image créée par KlingAI)