

Je reçois des notifications indésirables sur ma e-CPS. À quoi est-ce dû ?

Pour se connecter à un service numérique en santé (ex: Vaccin Covid, SI-DEP, etc.) par application mobile e-CPS, il faut saisir son identifiant RPPS au niveau du portail Pro Santé Connect. Cet identifiant est une donnée publique.

Cette saisie au niveau du portail déclenche une tentative d'authentification. Si le professionnel de santé concerné a activé sa e-CPS, alors une notification apparaît au niveau de son téléphone.

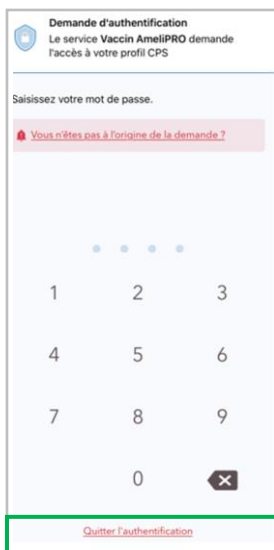
Un message, indiquant le service numérique cible est alors affiché. Pour valider la demande de connexion, il faut alors saisir son code PIN de e-CPS, à quatre chiffres, donnée personnelle et secrète.

Certains usurpateurs malveillants tentent d'abuser de la vigilance des professionnels de santé en déclenchant des notifications en espérant qu'ils les acceptent par réflexe ou pensant qu'il s'agit d'un collègue.

Il est très important de ne jamais valider une demande d'authentification dont vous n'êtes pas à l'origine. Cela pourrait conférer un accès en votre nom à un service numérique sensible et avoir des conséquences graves.

Que faire si je reçois une notification dont je ne suis pas à l'origine ?

Si vous recevez sur votre téléphone une demande d'authentification qui vous paraît suspecte, vous devez refuser l'accès (bouton 'refuser' de la notification ou bouton 'quitter l'authentification' dans l'application) ou ignorer la demande qui expirera au bout d'une minute.



Demande d'authentification
Le service Vaccin AmeliPRO demande l'accès à votre profil CPS

Saisissez votre mot de passe.

Vous n'êtes pas à l'origine de la demande ?

1 2 3
4 5 6
7 8 9
0

Quitter l'authentification



Vaccin AmeliPRO
Authentification pour le service Vaccin AmeliPRO

Refuser Accepter

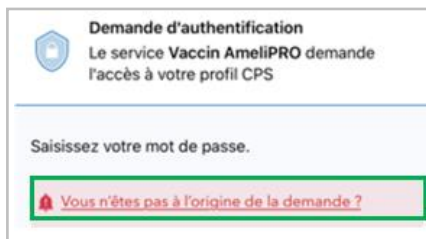
Que faire si je suis importuné régulièrement par des notifications de ce type ?

L'ANS met en œuvre des mécanismes pour bloquer les personnes malveillantes qui tentent de réaliser des notifications à répétition. Ces mécanismes ont été renforcés en février, et continueront de l'être dans les prochains mois, face à la recrudescence de telles pratiques.

Toutefois, si vous continuez d'être la cible de notifications indésirables, nous vous recommandons de **désactiver les notifications de l'application e-CPS dans les paramètres de votre terminal mobile**, en cliquant sur le bouton 'vous n'êtes pas à l'origine de la demande' puis en cliquant sur le bouton 'bloquer'. Cela nous aidera aussi à mieux identifier les tentatives malveillantes pour les bloquer à l'avenir.

Fiche pratique e-CPS – Hygiène numérique

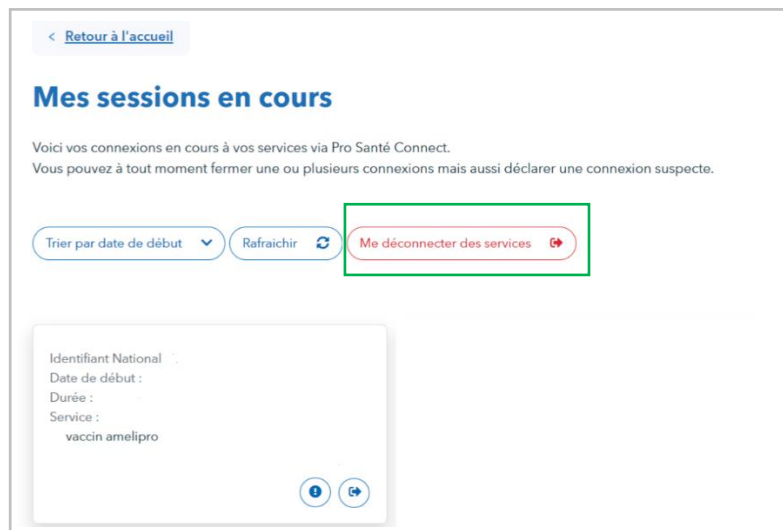
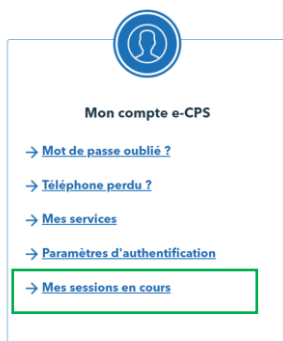
Je reçois des notifications indésirables sur ma e-CPS. Pourquoi ? Que faire ?



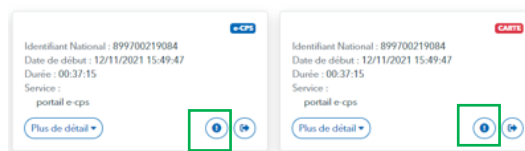
Cela ne vous empêchera pas d'utiliser votre e-CPS pour vos connexions légitimes, il suffira d'ouvrir l'application lorsque vous en avez besoin. Vérifiez bien qu'il s'agit du bon service puis validez alors votre demande d'authentification avec votre code PIN de e-CPS.

Que faire si jamais j'ai accepté par erreur une authentification ?

Dans ce cas, connectez-vous sur <https://wallet.esw.esante.gouv.fr/> et forcez la déconnexion de votre session Pro Santé Connect en cliquant sur l'icône de déconnexion rouge. Cela permettra à l'usurpateur d'être bloqué sur les services où il essaierait de se connecter en votre nom.



Au niveau de cette page récapitulant vos connexions, vous pourrez aussi identifier si une activité vous paraît suspecte.



Si vous vous en rendez compte trop tard, veuillez signaler cet incident auprès du support du service cible.

Dans quels cas dois-je faire un signalement ? À qui ?

En cas de notification indésirable sur votre e-CPS, il n'est pas nécessaire de le signaler. Le simple fait de refuser la connexion ou d'ignorer cette notification permet à l'ANS d'être au courant et de mieux prévenir d'éventuelles futures tentatives de ce type.

Si vous avez accepté une authentification par erreur, reportez-vous à la section ci-dessus.

Fiche pratique e-CPS – Hygiène numérique

Je reçois des notifications indésirables sur ma e-CPS. Pourquoi ? Que faire ?

Si vous suspectez, avec des éléments tangibles, que votre identité a été usurpée sur un service numérique en santé, quel qu'il soit (découverte de faux documents édités en votre nom, activité anormale détectée, etc.), alors contactez sans délai le service numérique concerné et portez plainte au commissariat de police, à la brigade de gendarmerie ou par écrit au procureur de la République du tribunal judiciaire dont vous dépendez. L'association France Victimes peut vous accompagner dans cette démarche au 116 006 (appel et services gratuits). Retrouvez plus d'informations sur l'usurpation d'identité en ligne à l'adresse <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite-que-faire#victime-usurpation-identite>.

Si vous avez découvert que vos coordonnées de contact (e-mail, téléphone mobile, adresse postale, etc.) référencées par votre ordre professionnel ont été modifiées à votre insu, contactez sans délai votre ordre professionnel pour faire les rectifications adéquates et déposez plainte via les moyens décrits ci-dessus. Ces coordonnées sont particulièrement importantes car elles sont utilisées pour l'activation des applications mobiles e-CPS et/ou la délivrance des cartes CPS. Toute modification de ces coordonnées doit faire l'objet d'une vérification de votre identité, ou d'une authentification renforcée.

Si j'ai un doute ou que j'ai besoin de plus d'explications sur le fonctionnement de Pro Santé Connect et de la e-CPS, qui contacter ?

Vous pouvez joindre le service support de l'Agence du Numérique en Santé au **0 809 40 00 82 (appel gratuit)** ou nous écrire par e-mail sur monserviceclient.e-cps@asipsante.fr.

Pour les professionnels libéraux, vous pouvez également en parler avec vos conseillers informatique services.

À propos de Pro Santé Connect

Pro Santé Connect est une solution de l'Agence du Numérique en Santé, pour simplifier et sécuriser la connexion des professionnels aux services numériques en santé. Elle a déjà été adoptée comme mode de connexion par une centaine de services numériques en santé. Elle recense chaque mois environ 10 millions d'authentifications, à 60% par e-CPS, et à 40% par CPS.