Session informatique du 3 octobre 2022

Sécurité Windows et Internet

Ordre du jour

- Menaces sur Internet et protections à adopter
- Comptes Windows et droits
- Sécurité du compte Windows

Menaces sur Internet et précautions à adopter

- Adresse mail compromise
- Spam
- Hameçonnage (Pishing)
- Sites frauduleux

Adresse mail compromise

Cause: site internet piraté sur lequel vous avez un compte (adresse mail, mot de passe)

Alerte: le propriétaire du site averti les propriétaires des comptes piratés

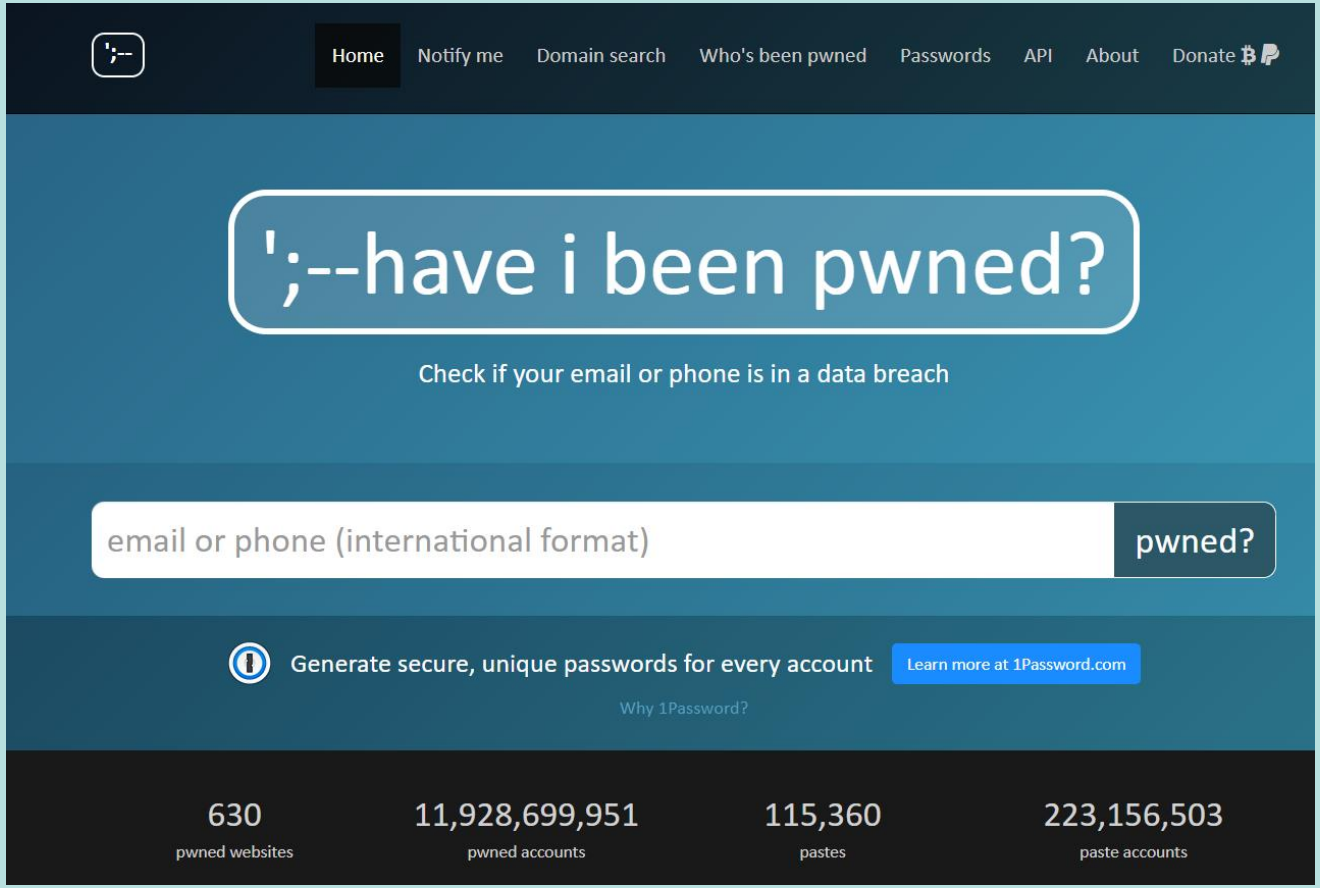
Remède: changer le mot de passe associé à l'adresse mail du compte et sur tous les sites ou le couple adresse mail/mot de passe a été enregistré.

Comment savoir si son adresse mail a été compromise:

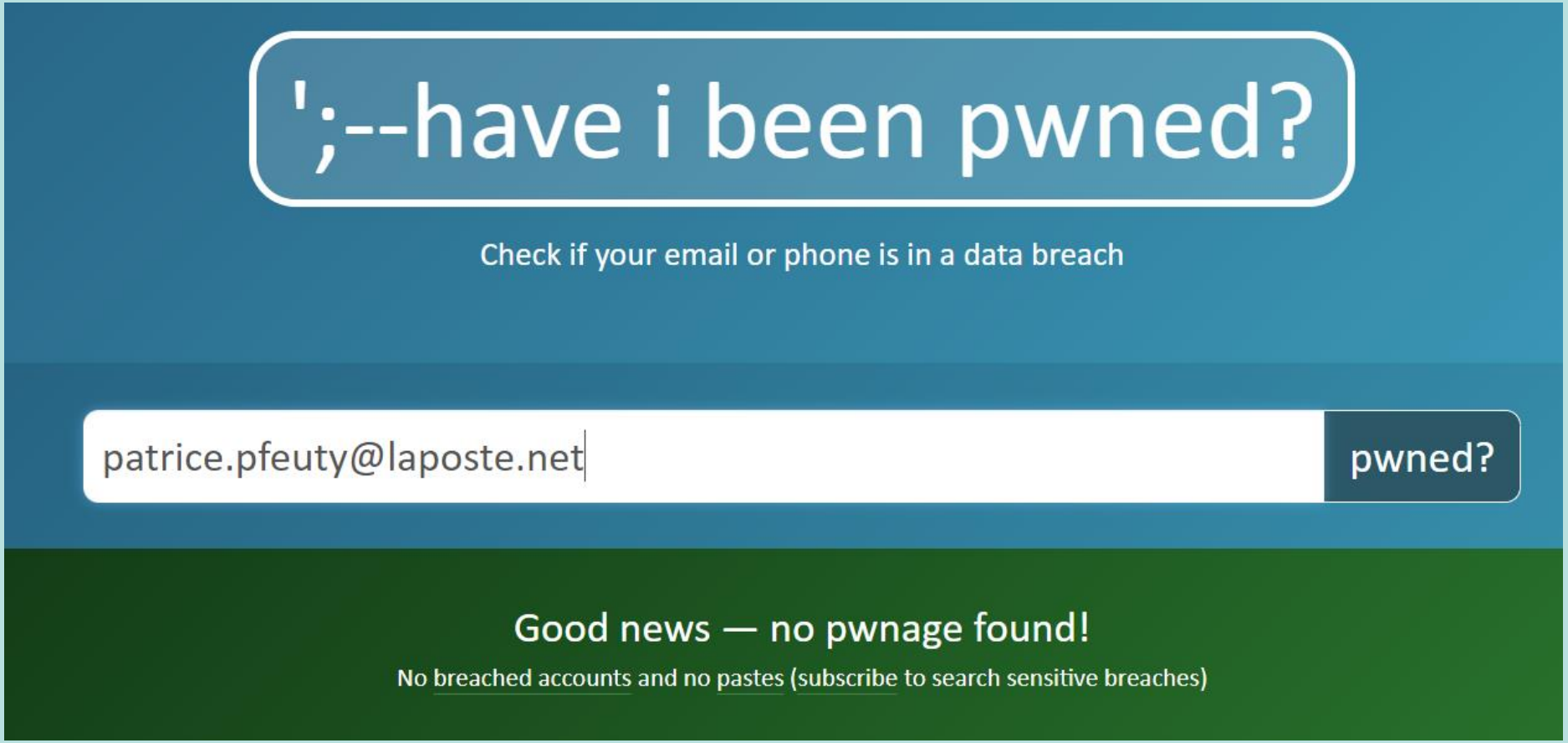
Vérifier sur le site suivant:

https://haveibeenpwned.com

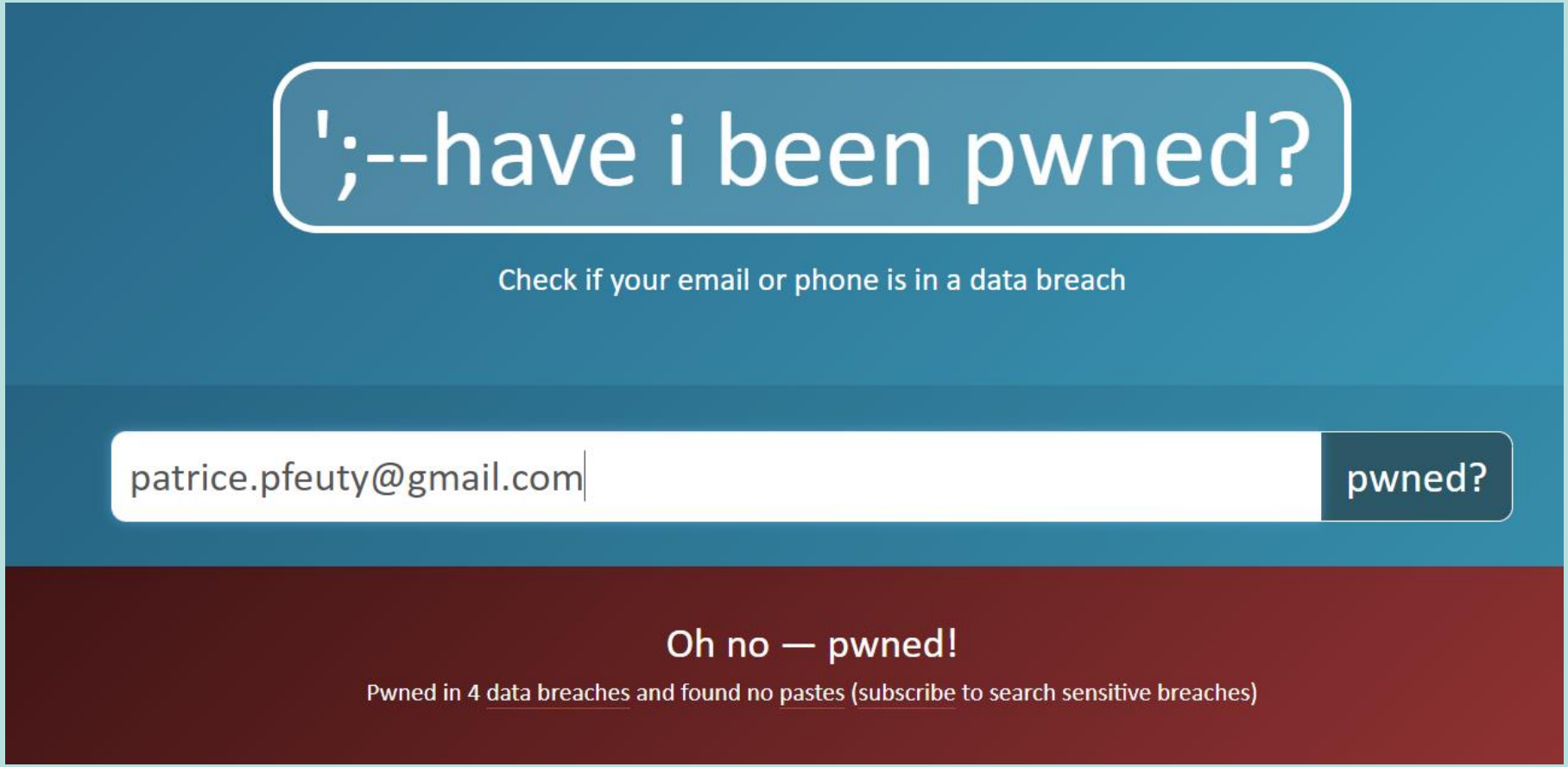
Vérification d'adresse mail



Adresse non compromise



Adresse mail compromise



Sites piratés responsables de l'adresse compromise

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Cit0day (unverified)**:** In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames

Spam

- Spam : mail non sollicité
- Spam sans risque: lettre d'information suite à l'enregistrement de son adresse mail sur un site Internet
  - Remède: se désabonner de la lettre d'information en cliquant sur le lien « se désabonner » ou « unsubscribe » (sites étrangers)
  - Utiliser une seconde adresse mail (« poubelle »)
  - Utiliser une adresse mail provisoire: https://temp-mail.org/fr/
- Spam avec risque: message frauduleux cherchant à récupérer des données confidentielles sensibles (numéro de carte bancaire…) ou demandant de verser de l'argent pour différentes raisons
  - Précaution: ne pas cliquer sur les liens proposés dans le mail (risque d'hameçonnage)
  - Ne pas cliquer sur les pièces-jointes: risque d'installation d'un virus
  - Supprimer le mail

Hameçonnage

Un lien Internet renvoie vers un faux site (copie d'un site réputé) pour capturer des informations sensibles

Lien Internet:

- texte du lien : affiché
- adresse Internet: adresse du site (masquée) associée au texte

Comment vérifier si un lien Internet présente un risque:

https://www.virustotal.com/gui/home/url

Réputation des sites Internet

En cas de doute sur une offre alléchante ou un site douteux, il est recommandé de consulter les sites suivants:

Signal-Arnaques | Plateforme de signalements d'arnaques

Installer l’extension France Verif

FranceVerif - Microsoft Edge Addons

Vérifier les avis avec Trust Pilot: !

Avis Trustpilot - Découvrez le pouvoir des avis clients

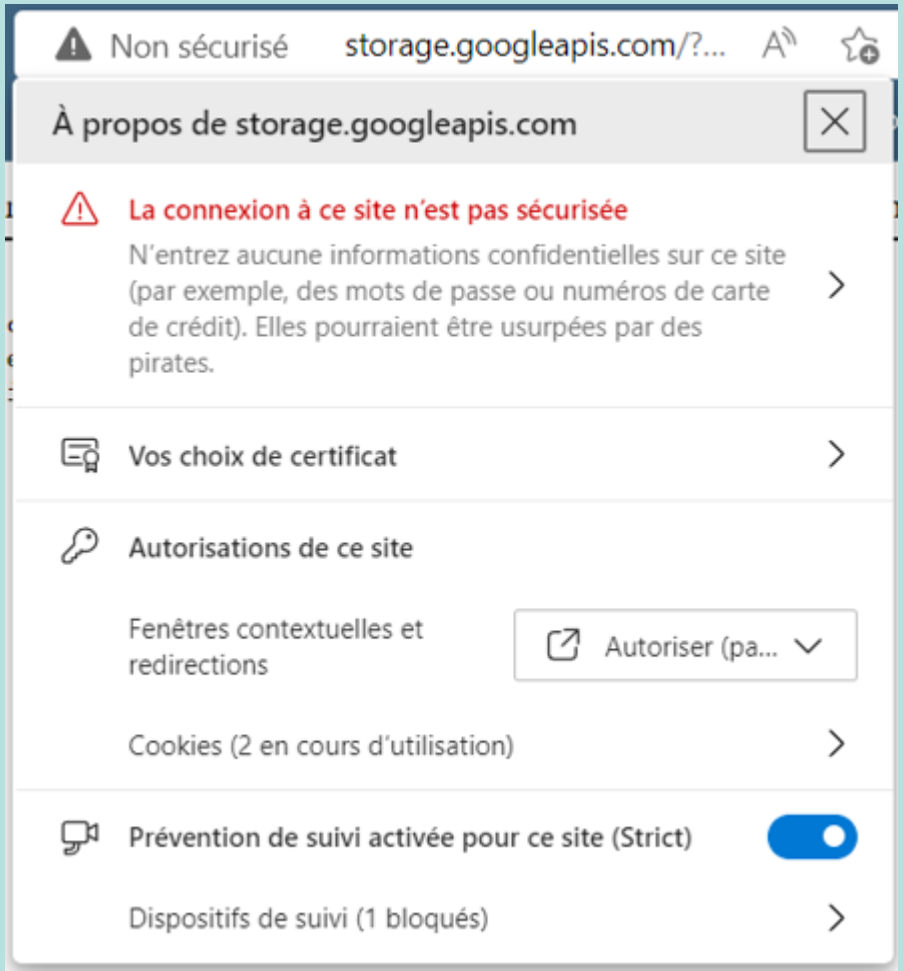
Vérification d’adresse mail

Scamdoc.com | Check if a website is legit or not

Sécurité des sites Internet

Pour acheter sur Internet, vérifier que le site est sécurisé:

L’adresse du site doit commencer par http**s**



Naviguer en sécurité avec Microsoft Edge

Paramètres / Sécurité Windows

Contrôle des applications et du navigateur

Protection d'applications et sécurité en ligne.

Protection fondée sur la réputation

Ces paramètres protègent votre appareil contre les applications, les fichiers et les sites web malveillants ou potentiellement indésirables.

Application potentiellement indésirable détectée. Votre appareil peut présenter des performances médiocres.

Révision

Paramètres de protection fondée sur la réputation

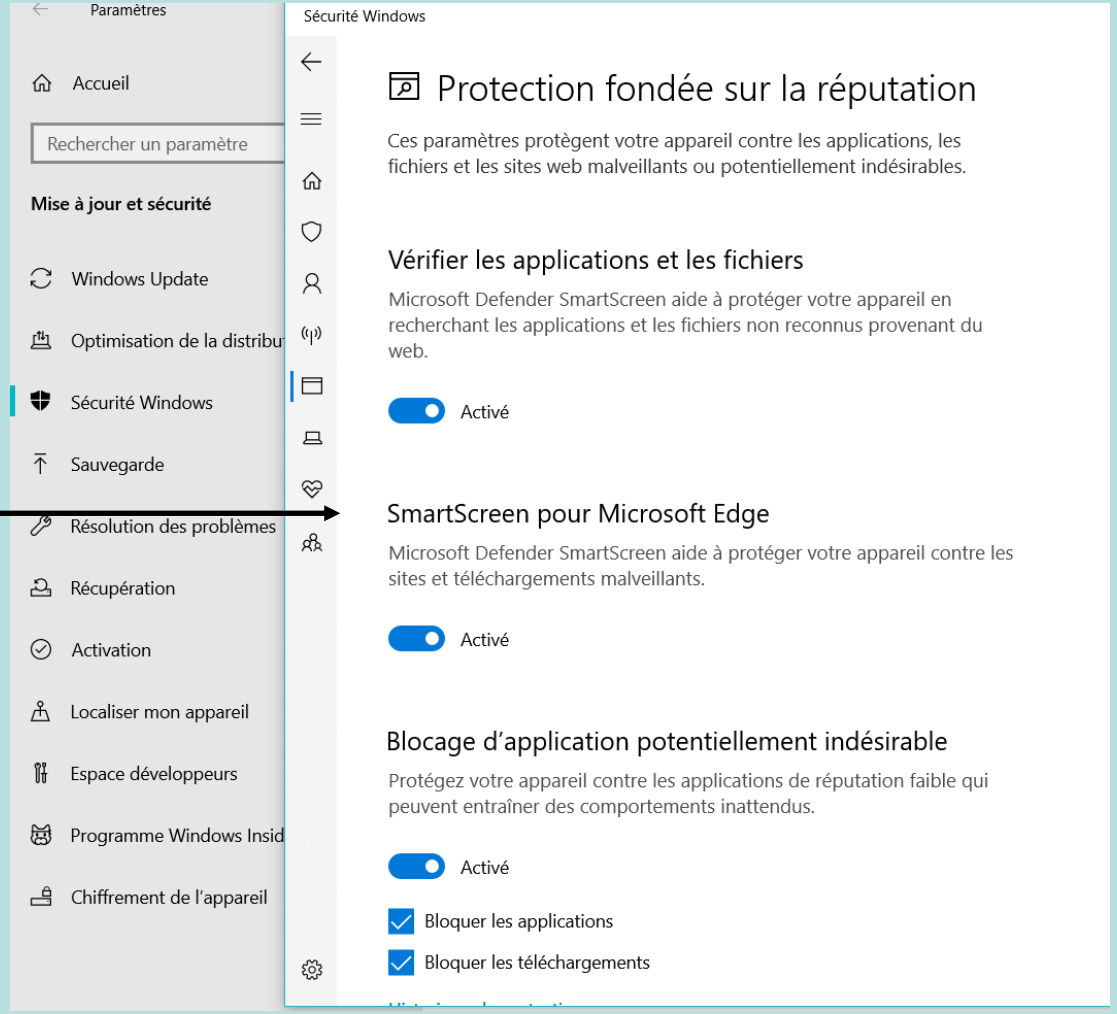
Ignorer

Exploit protection

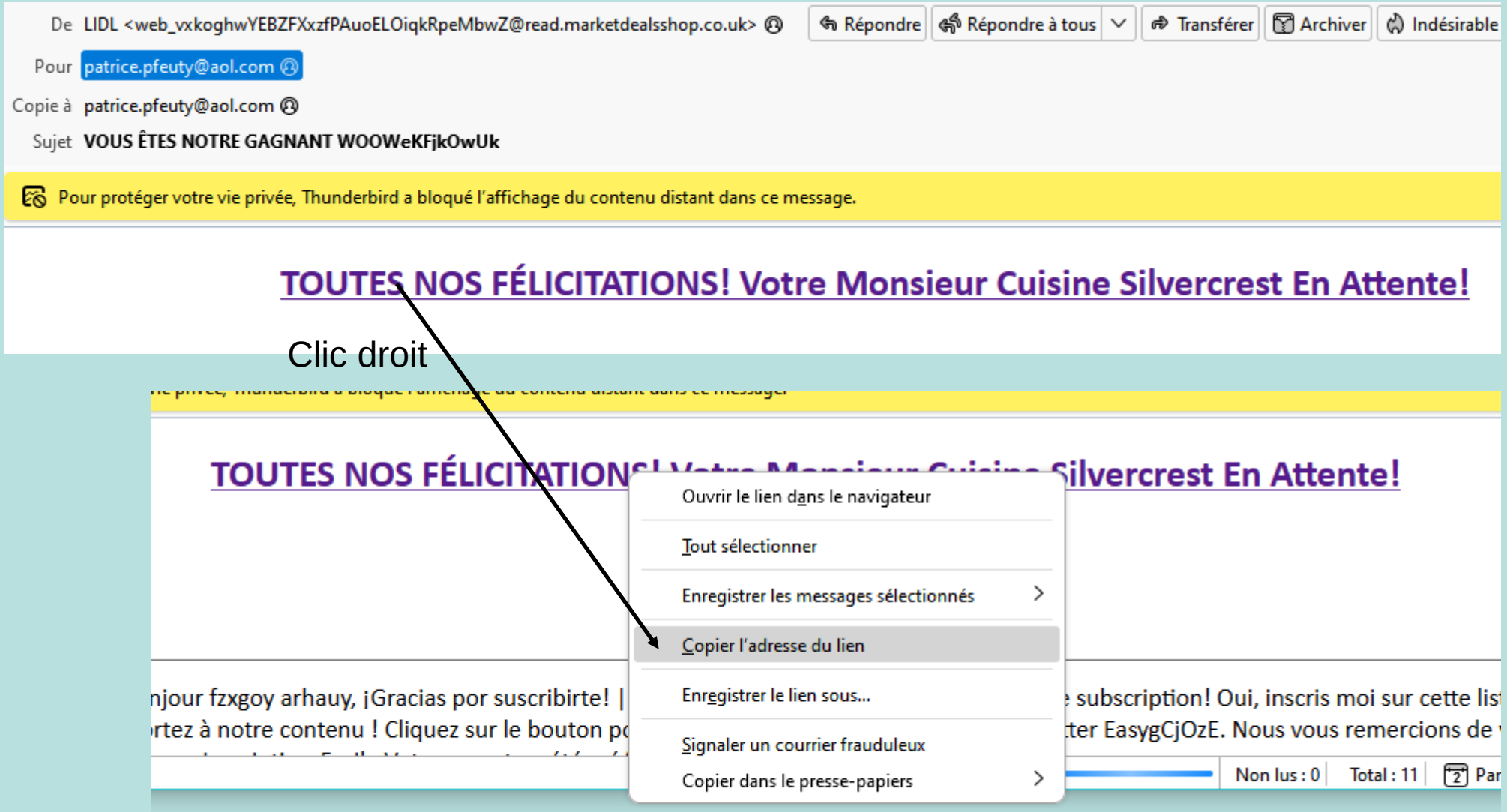
Exploit protection est intégré à Windows 10 pour protéger votre appareil contre les attaques. Dès sa sortie de l'emballage, l'appareil est déjà configuré avec les paramètres de protection qui fonctionnent le mieux pour la plupart des utilisateurs.

Paramètres d'Exploit protection

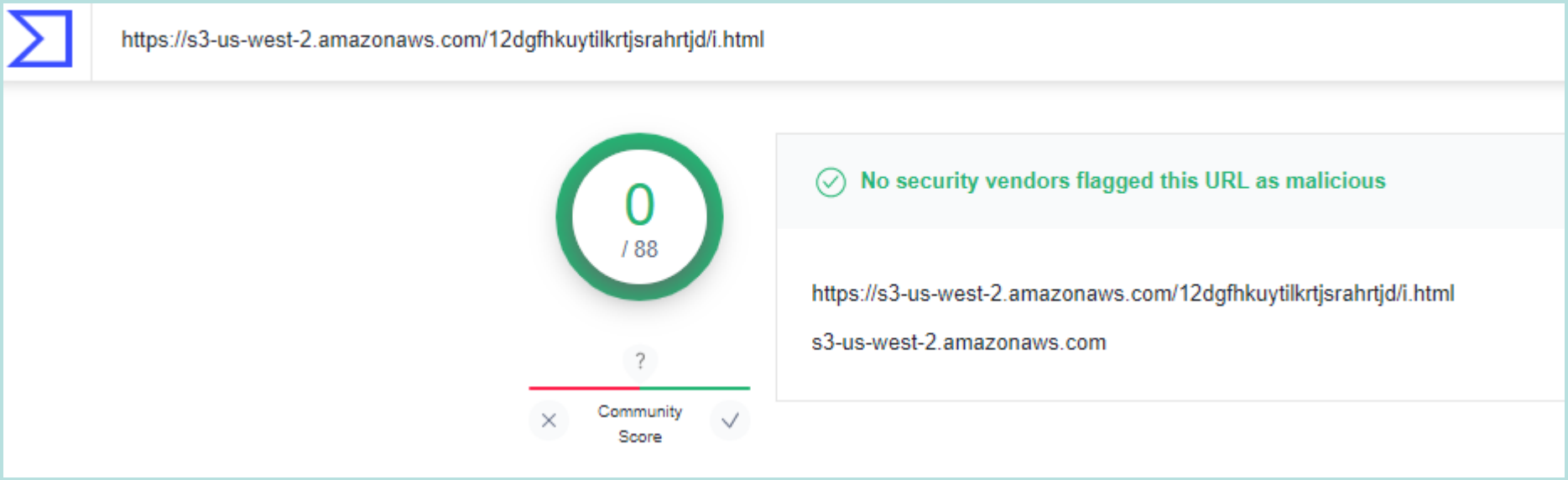
En savoir plus



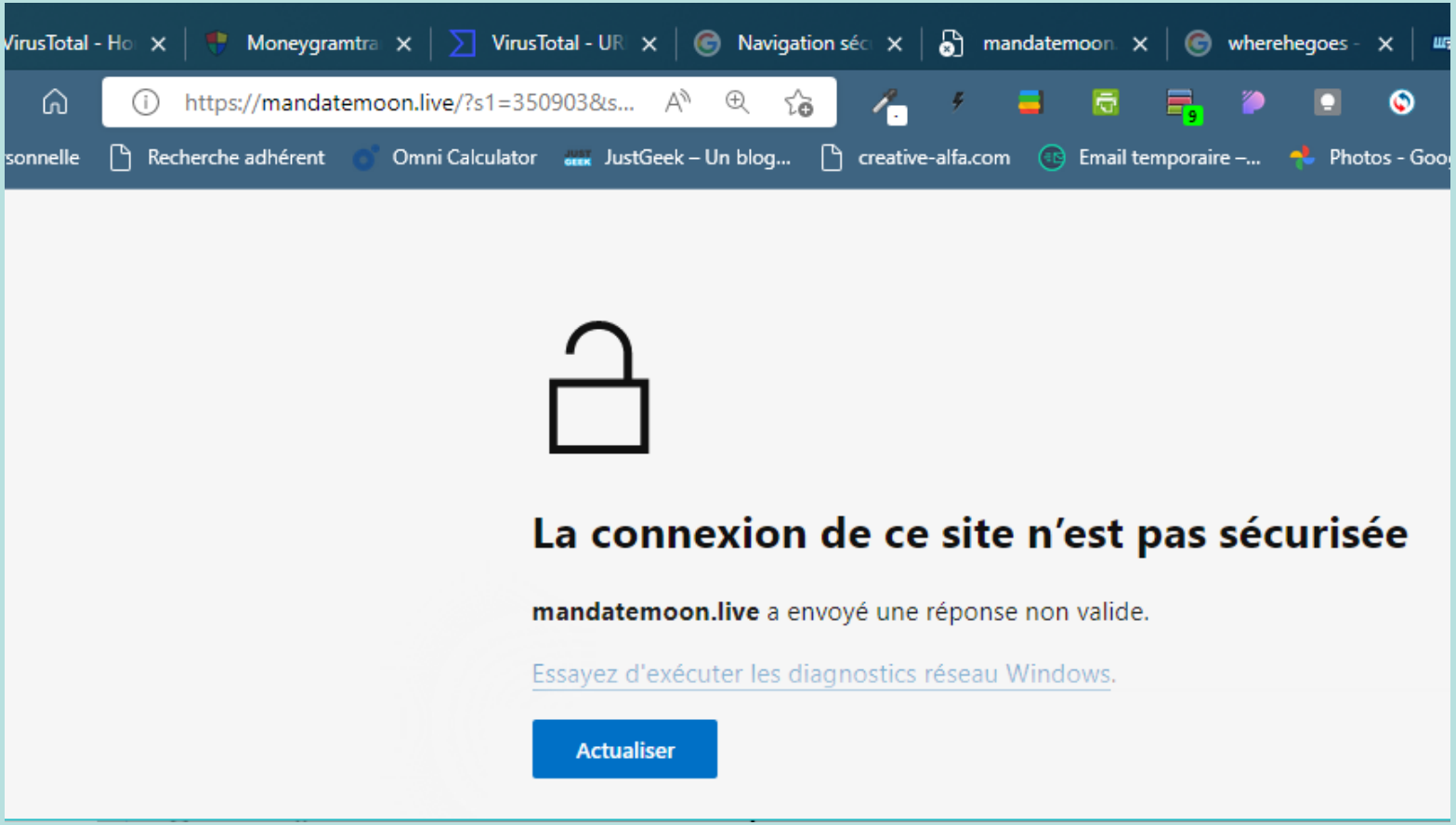
Spam avec risque d'hameçonnage



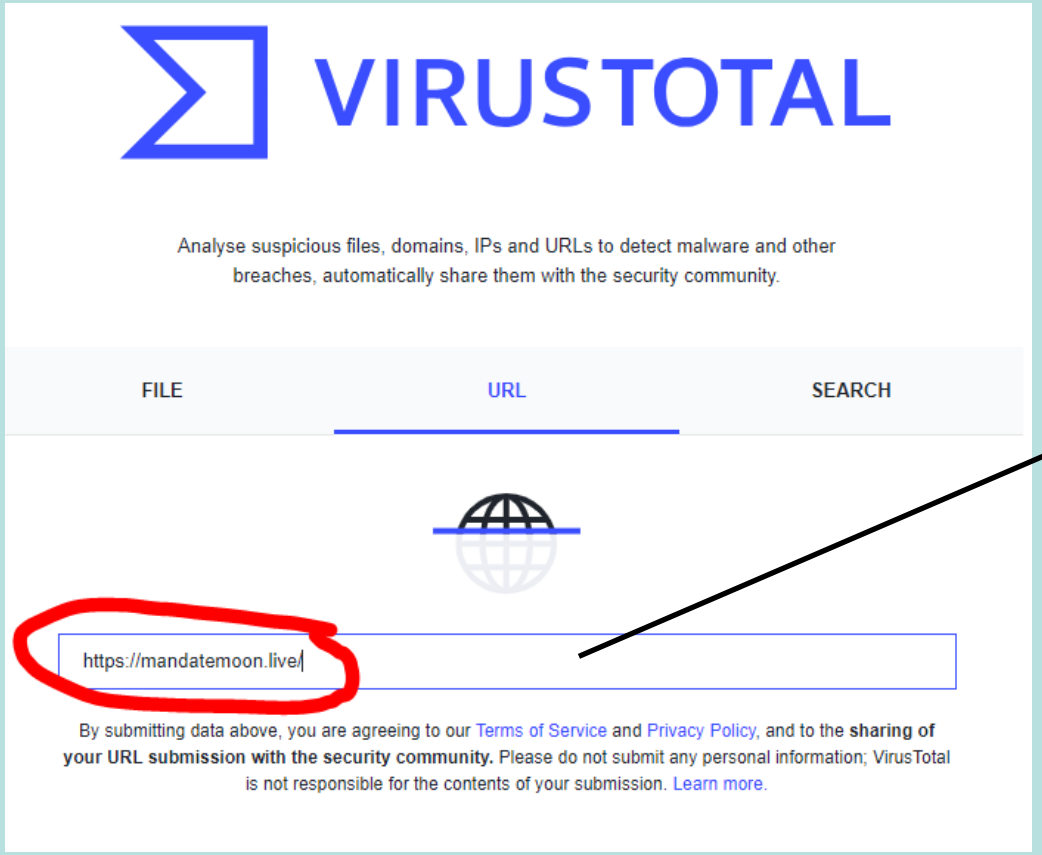
Contrôle d’url avec VIRUSTOTAL

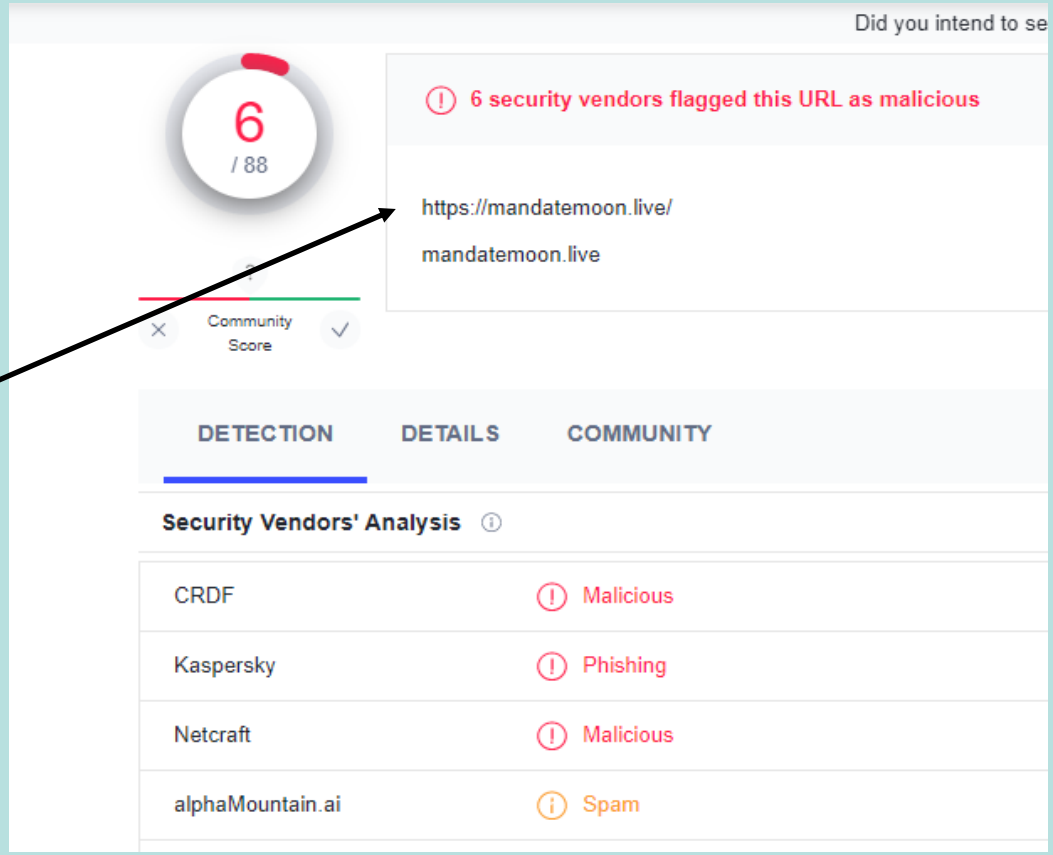


Blocage du site par Edge (SmartScreen)

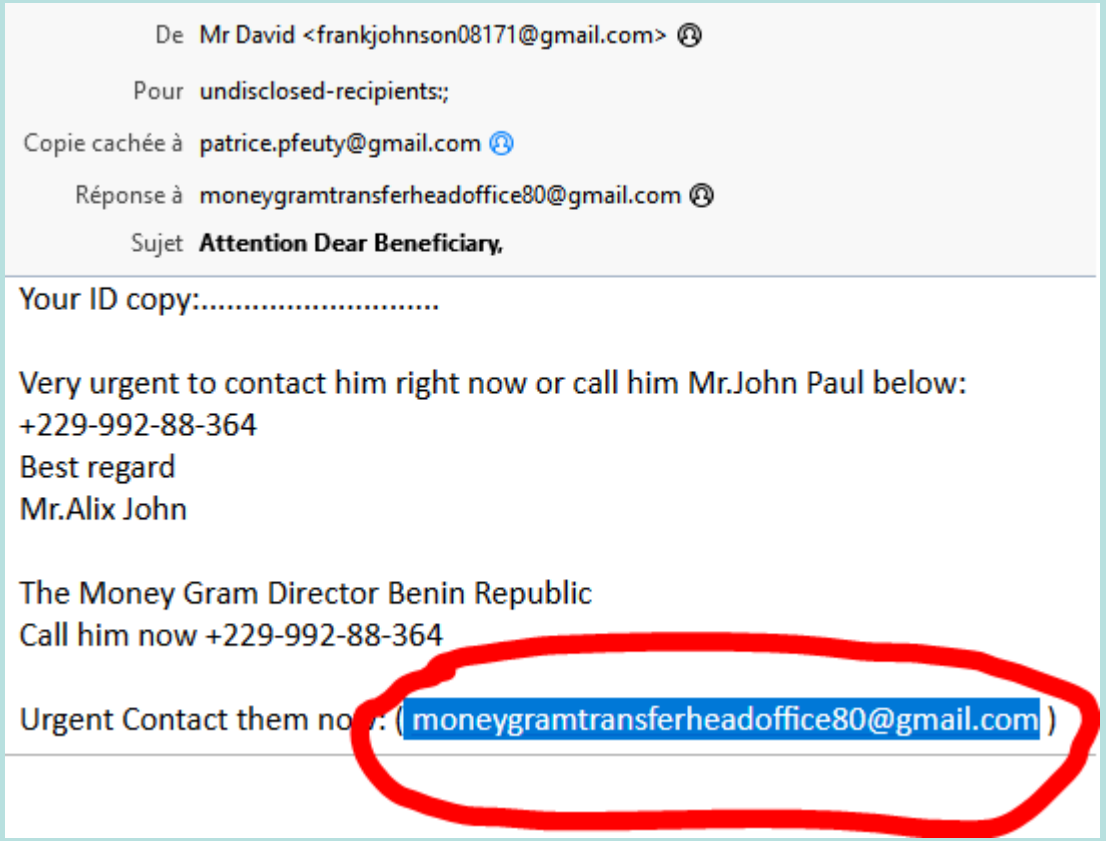


Contrôle de l'URL avec VIRUSTOTAL





Vérification d'adresse mail



De Mr David <frankjohnson08171@gmail.com>
Pour undisclosed-recipients:;
Copie cachée à patrice.pfeuty@gmail.com
Réponse à moneygramtransferheadoffice80@gmail.com
Sujet **Attention Dear Beneficiary,**

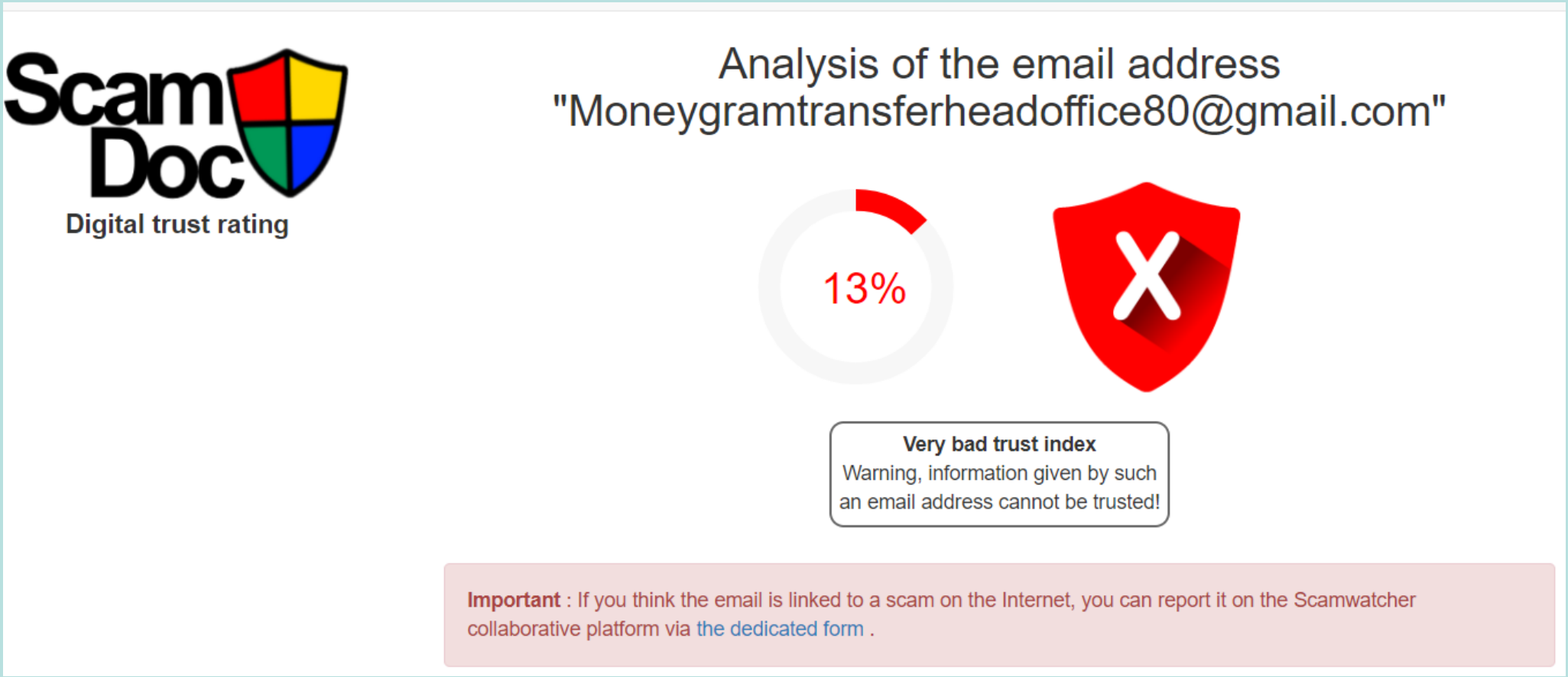
Your ID copy:.....

Very urgent to contact him right now or call him Mr.John Paul below:
+229-992-88-364
Best regard
Mr.Alix John

The Money Gram Director Benin Republic
Call him now +229-992-88-364

Urgent Contact them now: (moneygramtransferheadoffice80@gmail.com)

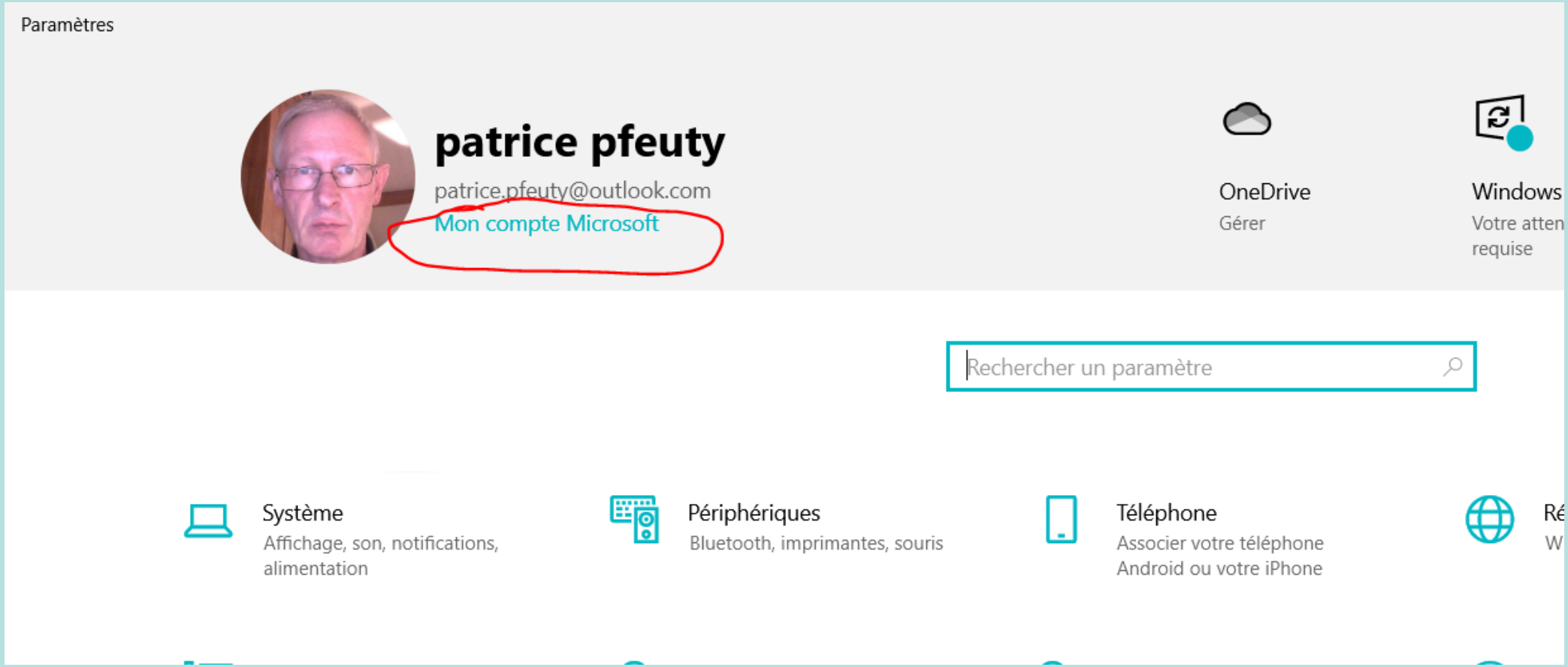
Vérification d’adresse mail avec ScamDoc



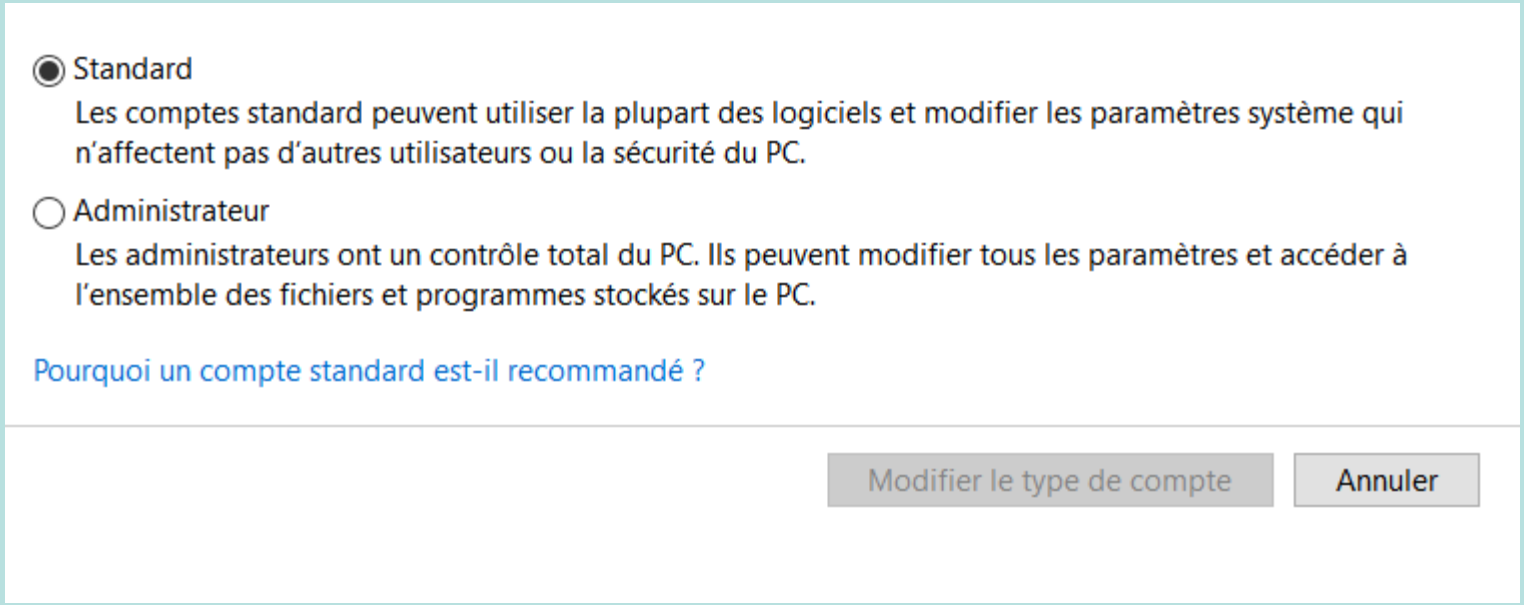
Comptes Windows

- Compte = identifiant + mot de passe + type de compte
- Types de compte Windows
  - Local (hors connexion) ou Microsoft (adresse mail)
  - Administrateur ou standard (interdiction d’installer des logiciels)

Type de compte Microsoft



Type de comptes standard ou Administrateur

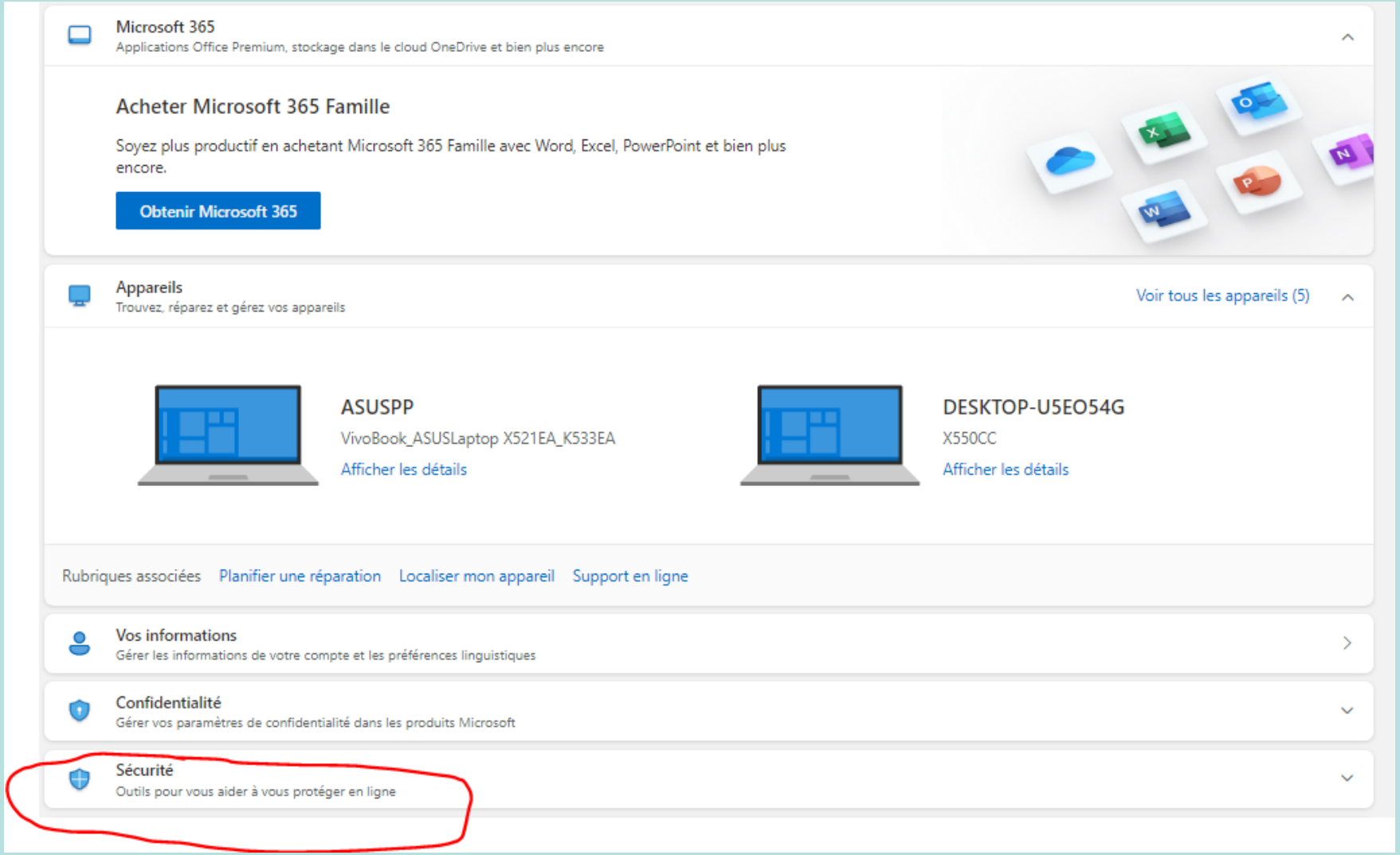


Paramètres du compte Microsoft

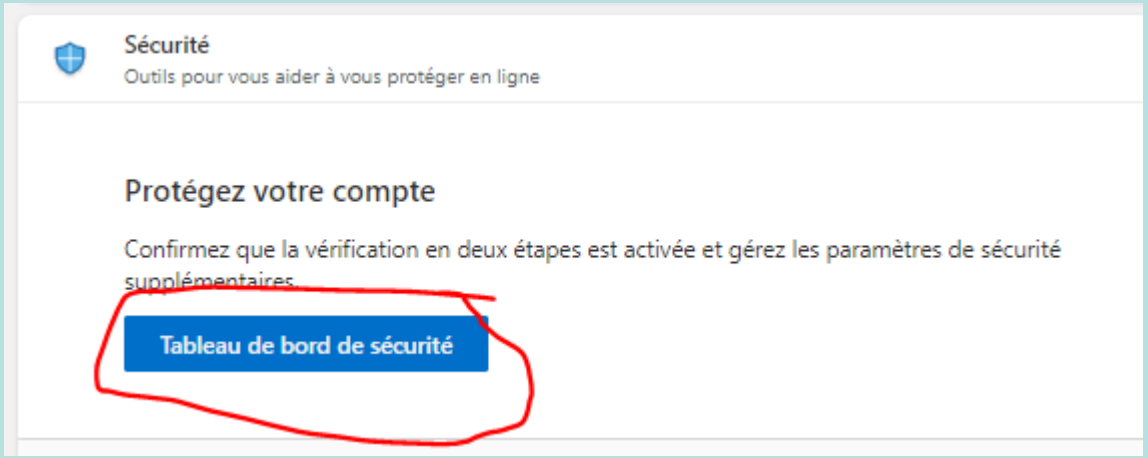
Paramètres Windows (+ I)

Cliquer sur le lien Mon compte Microsoft

Sécurité du compte Microsoft

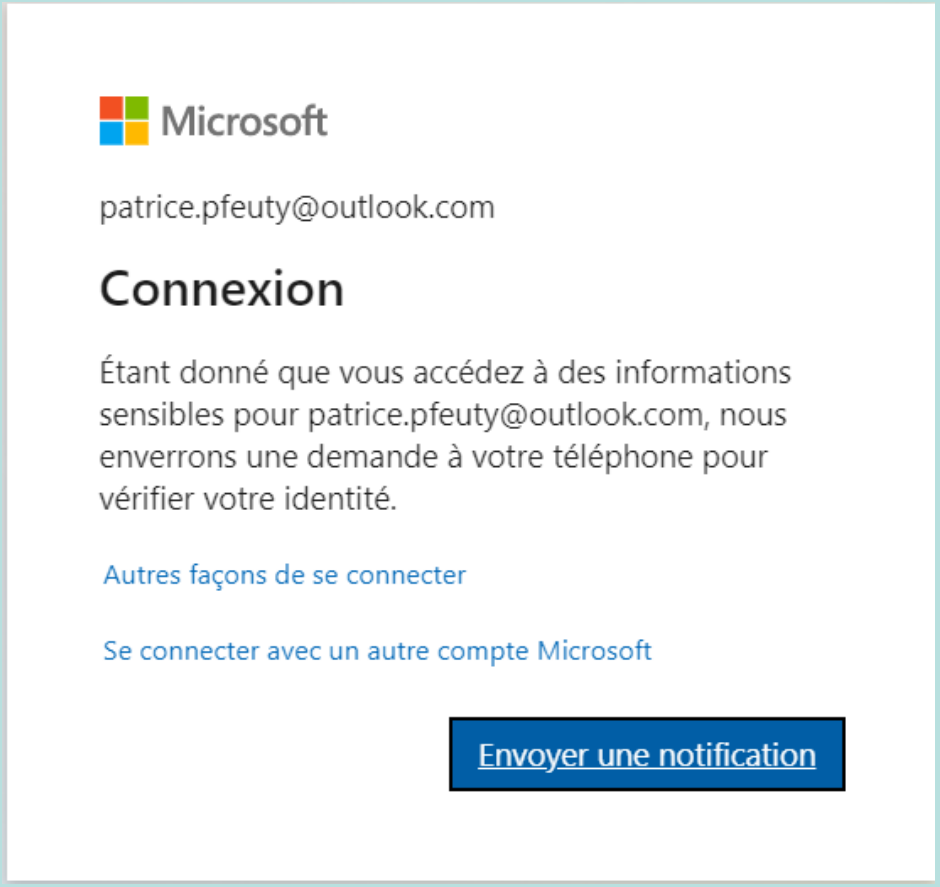


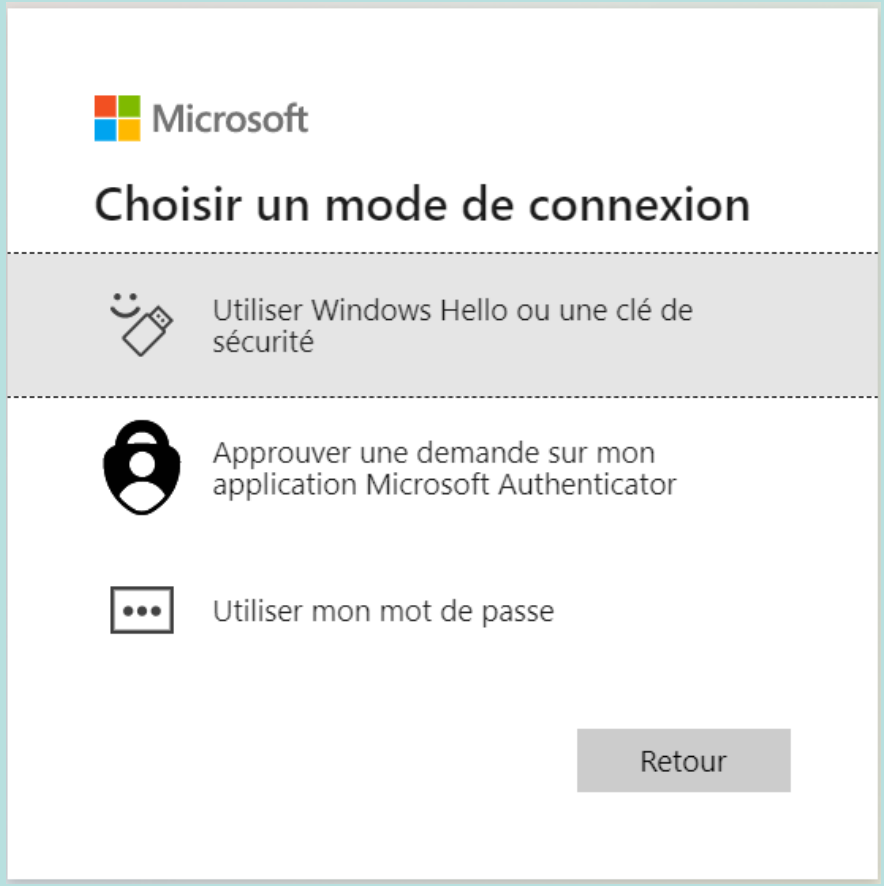
Sécurité du compte Microsoft



Accès à la sécurité du compte Microsoft

La sécurité étant un élément sensible, une authentification est nécessaire pour accéder au tableau de bord de sécurité du compte Microsoft





Authentification avec Microsoft Authenticator sur smartphone

Sécurité avancée

Sécurité

Modifier le mot de passe
Modifié: 21/08/2015

Vérification en deux étapes
Activer

Notion de base sur la sécurité

Gérez votre mot de passe, protégez votre compte et consultez des ressources de sécurité supplémentaires.

Activité de connexion

Vérifiez où et quand vous vous êtes connecté et dites-nous si quelque chose vous semble inhabituel.

Consulter mon activité

Sécurité du mot de passe

Aidez à sécuriser votre compte en utilisant un mot de passe plus fort.

Changer mon mot de passe

Options de sécurité avancées

Essayez les dernières options de sécurité pour sécuriser votre compte.

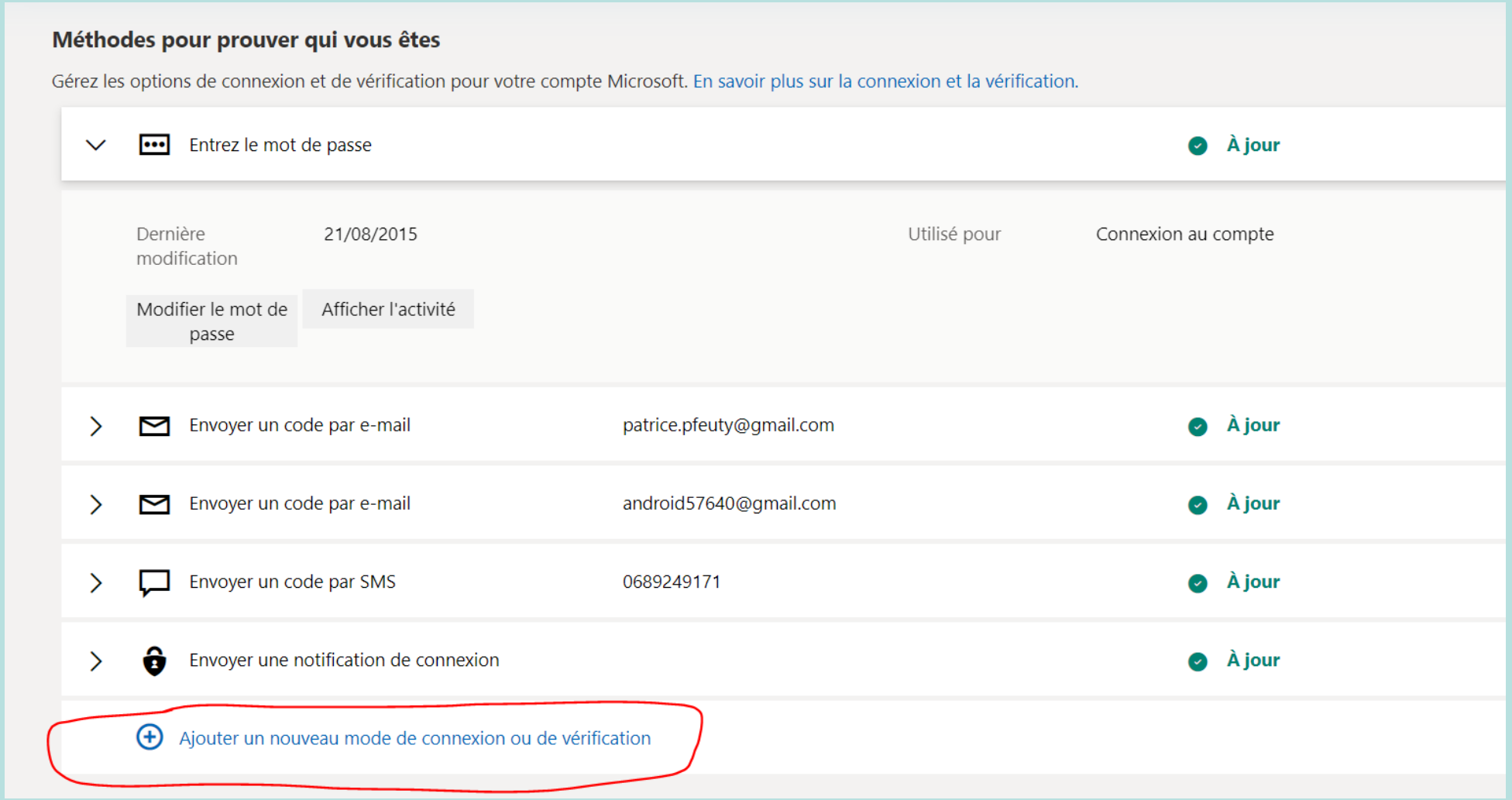
Prise en main

Assurer votre sécurité avec...

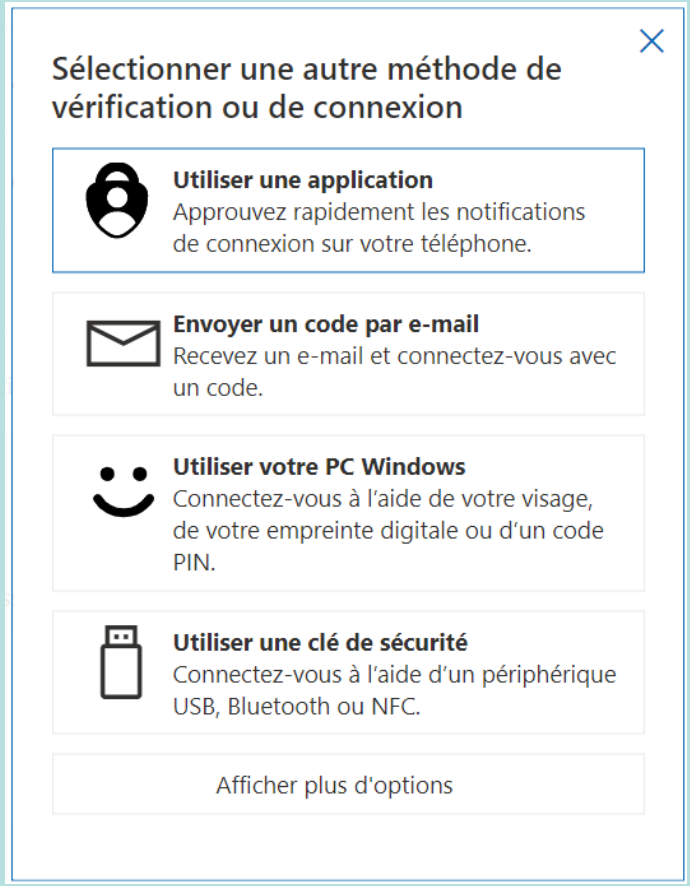
Windows 10 permet de rester plus facilement en sécurité grâce à une protection intégrée utilisant l'antivirus Microsoft Defender.

Vérifiez la sécurité de Windows

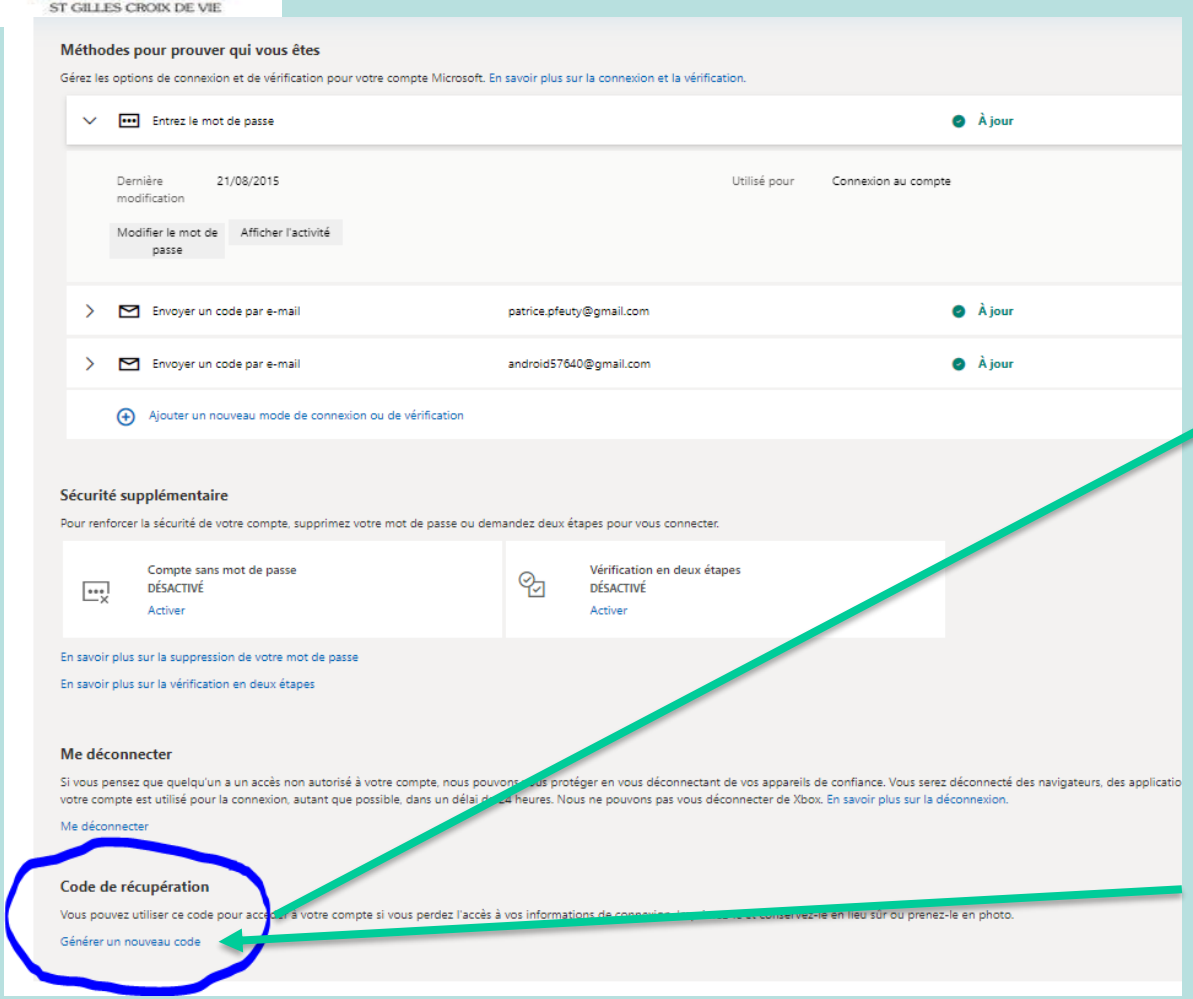
Méthodes d'authentification

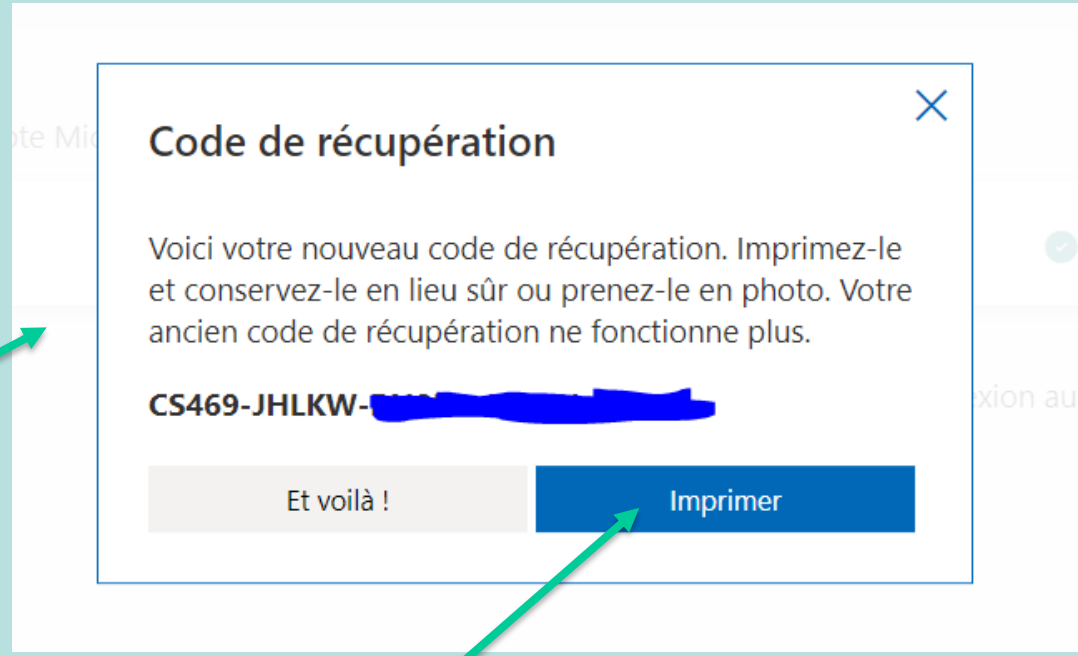


Méthodes d’authentification



Code de récupération du compte





Cliquer sur
Générer un nouveau code puis sur **Imprimer**

Code de récupération

Compte Microsoft

Voici votre nouveau code de récupération. Si vous devez récupérer l'accès à votre compte, ce code vous sera utile. Imprimez-le ou écrivez-le et conservez-le en lieu sûr. Nous vous recommandons fortement de ne pas stocker votre code de récupération sur un appareil.

Si vous disposiez précédemment d'un code de récupération, celui-ci n'est plus valide. Utilisez ce nouveau code à la place.

Votre nouveau code est **CS469-JHLKW-BN8BA-**[redacted]

Créé le : 25/04/2022 05:16:53 (UTC)

Pour le compte : pa*****@outlook.com

Réduire les droits du compte Windows principal

Objectif: interdire l'installation de logiciels malveillants

Procédure:

- Créer un compte local de type *administrateur* (2 méthodes possibles) *et* **conserver le mot de passe en lieu sur.**
- Se connecter avec le compte administrateur nouvellement créé
- Changer le compte principal en type de compte standard
- Se déconnecter du compte administrateur et se reconnecter à son compte principal

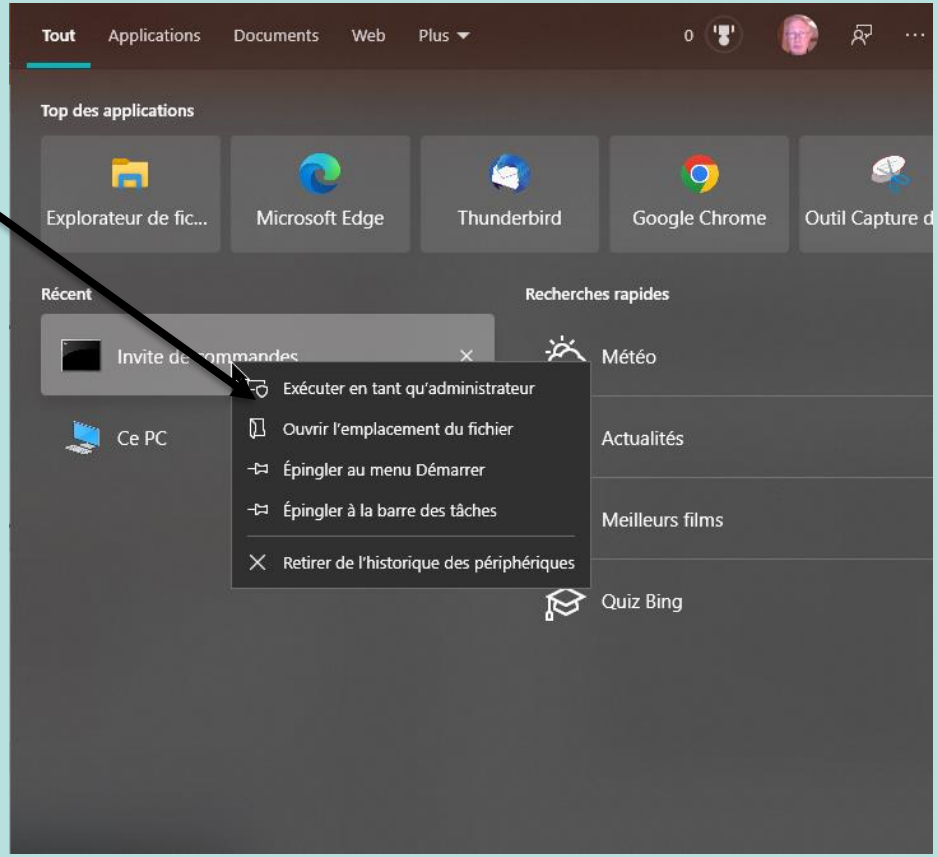
Utilisation:

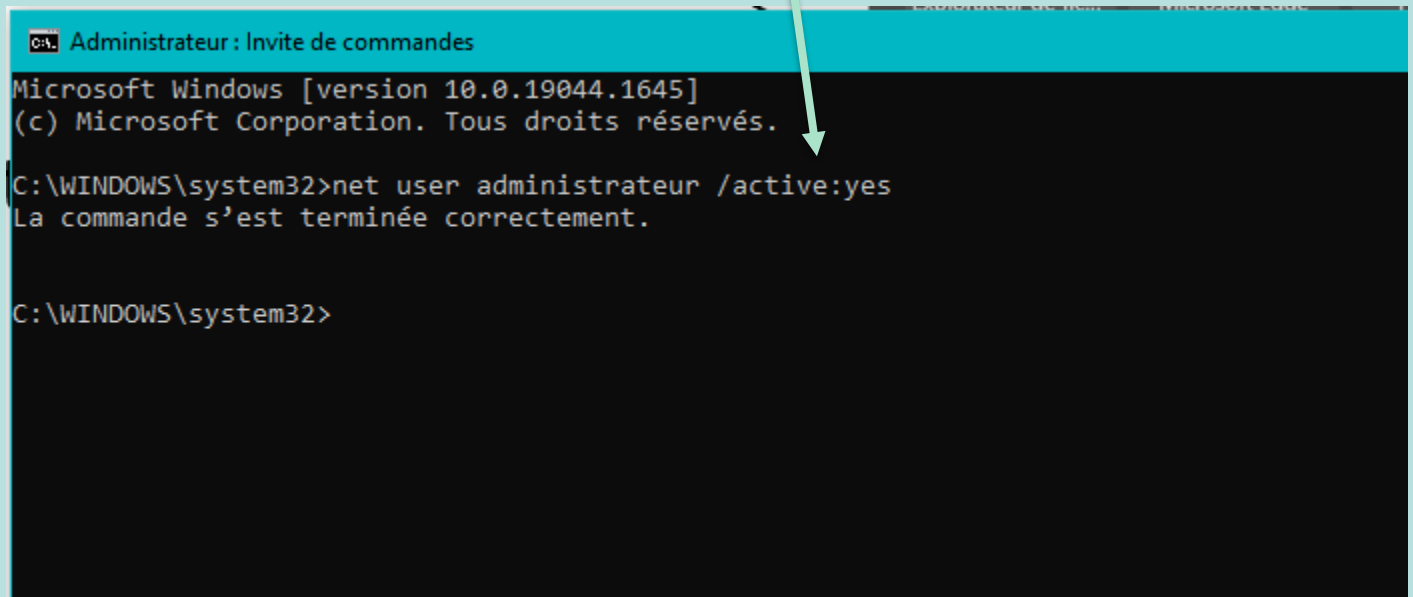
Chaque opération nécessitant le droit administrateur ouvrira une fenêtre de dialogue demandant le mot de passe utilisateur

Méthode 1 - Activer le compte administrateur existant

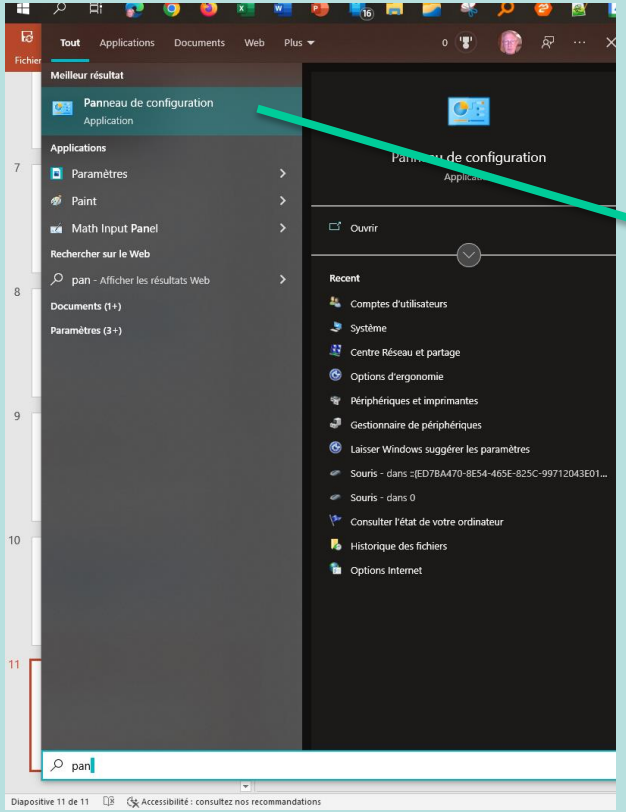
Commande en mode administrateur

Net user administrateur /active:yes

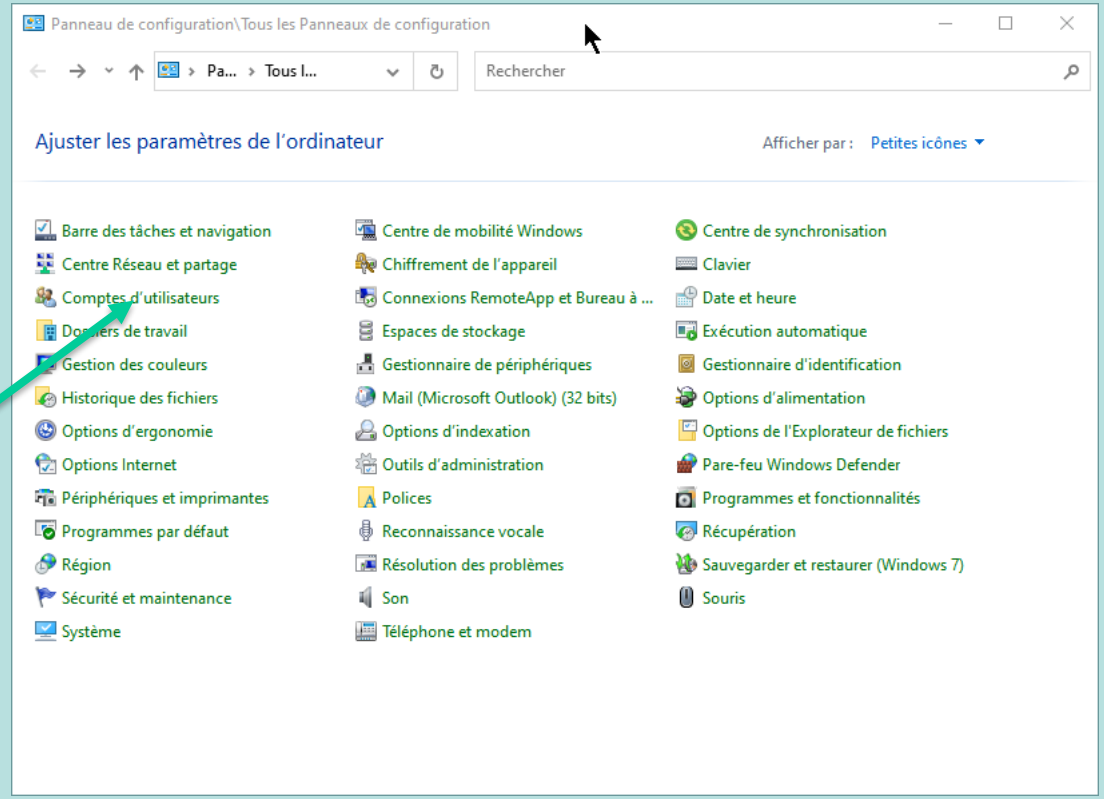




Méthode 1- définir le mot de passe du compte administrateur

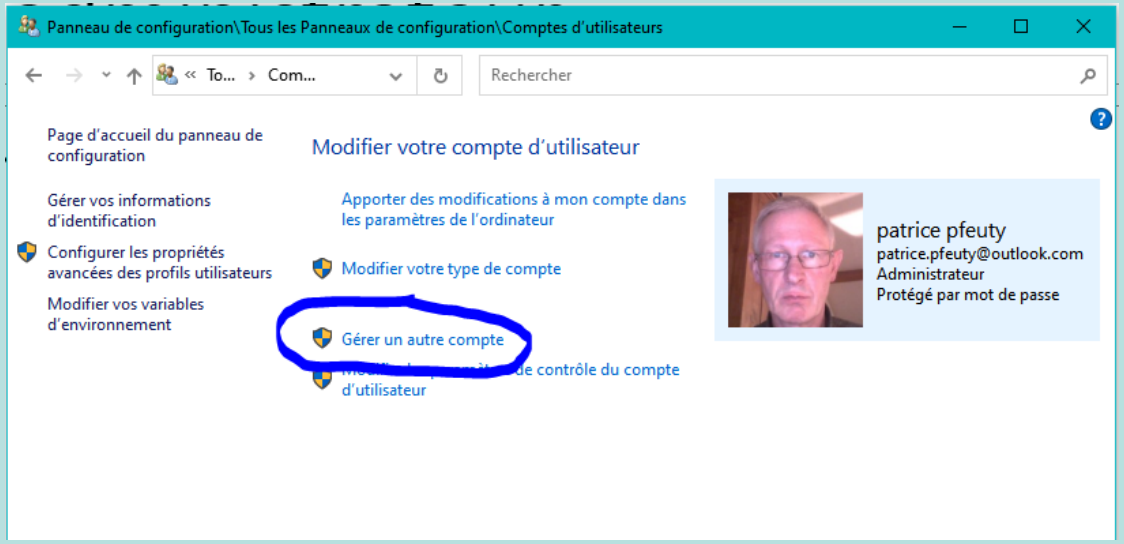


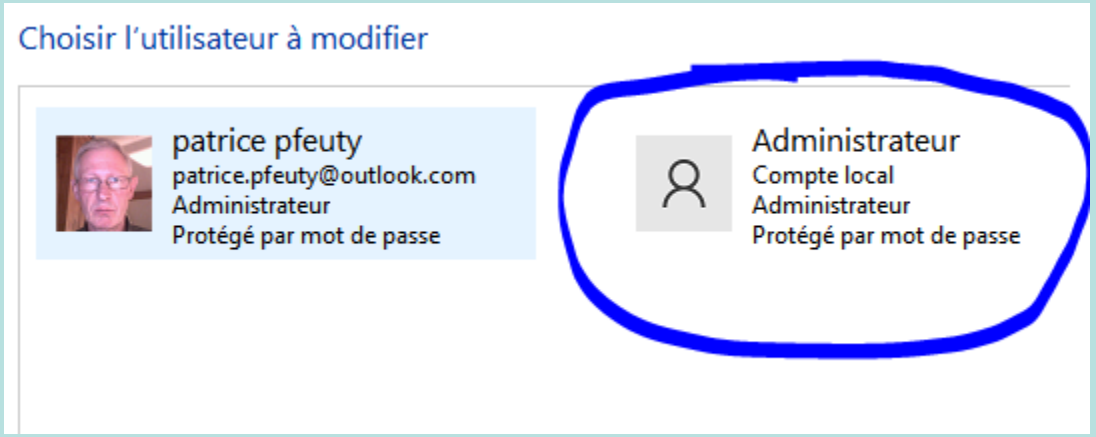
Comptes d'utilisateurs



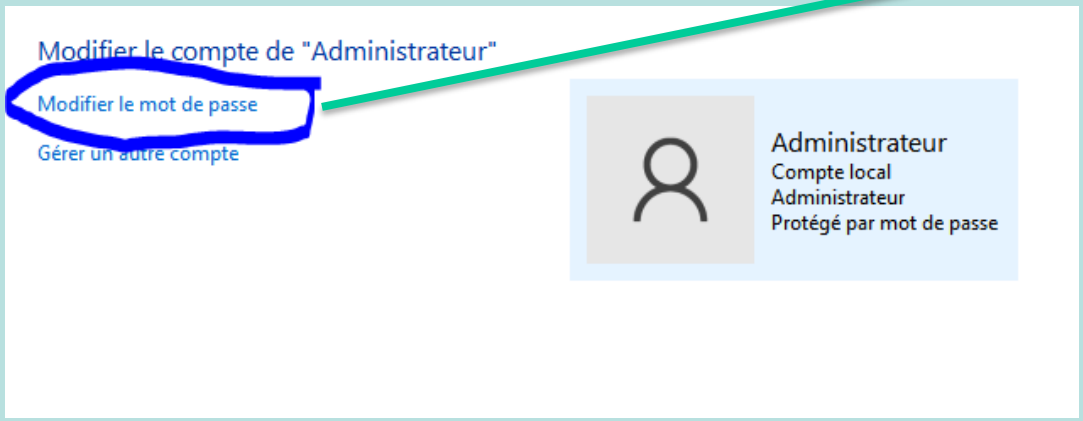
Méthode 1 - Définir ou modifier le mot de passe du compte administrateur

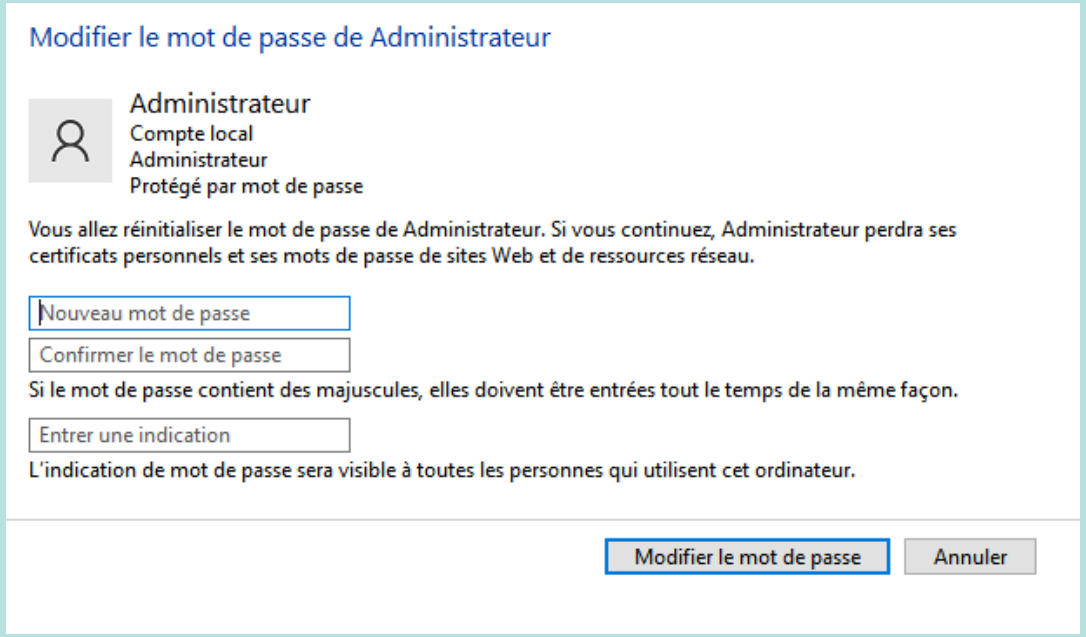
Saisir le mot de passe





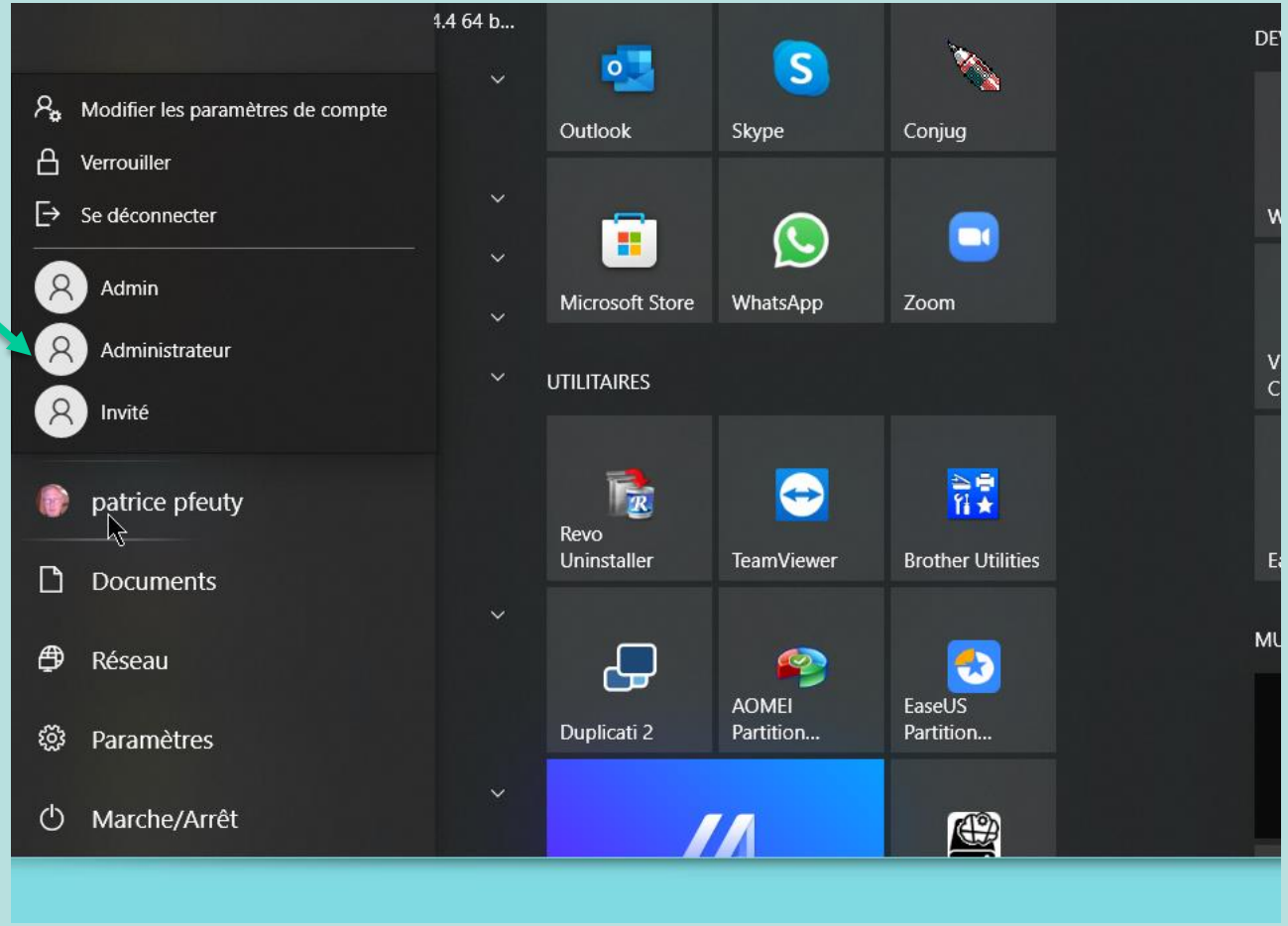
Méthode 1- Définir ou modifier le mot de passe du compte administrateur





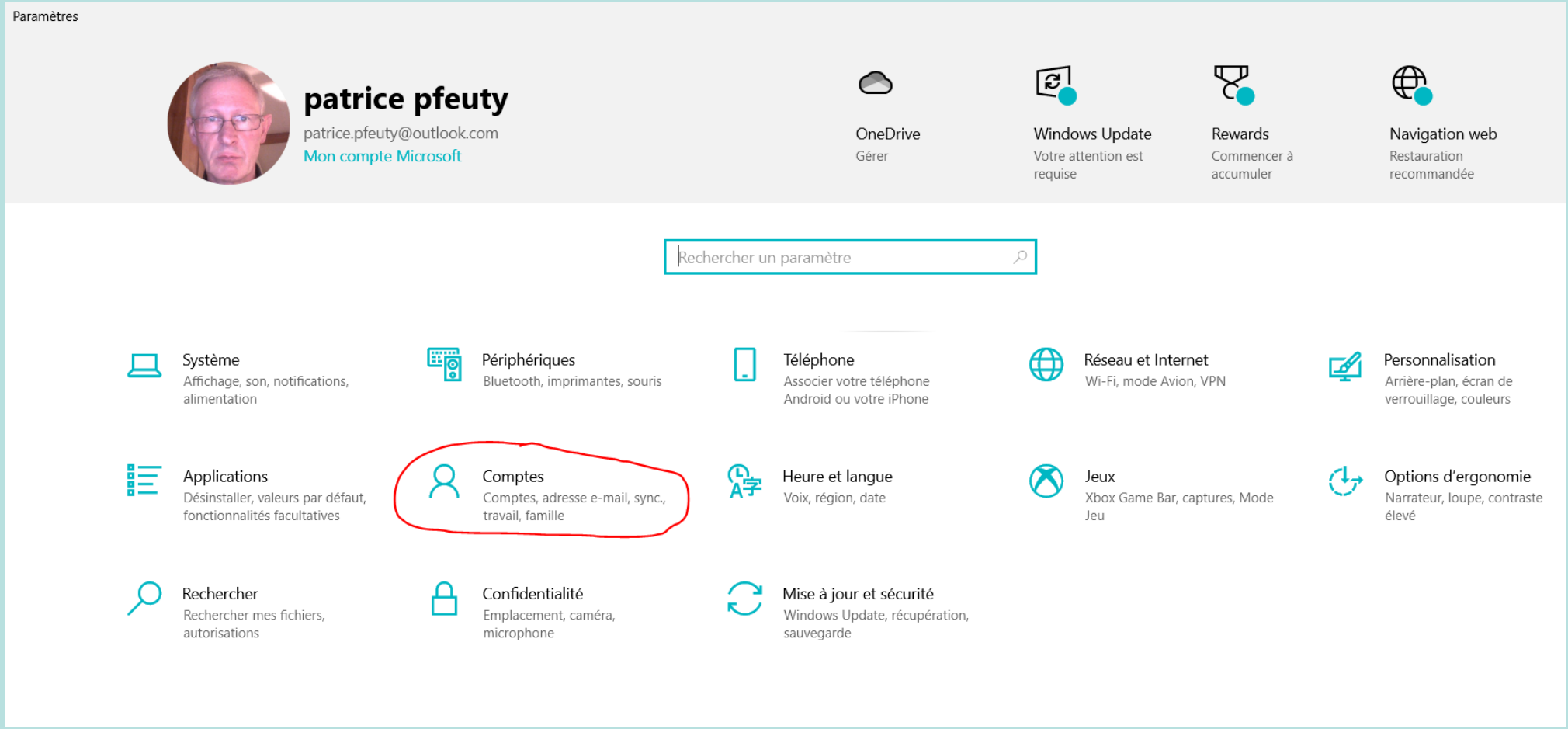
Méthode 1 - Utiliser le compte administrateur

Compte Admininstrateur

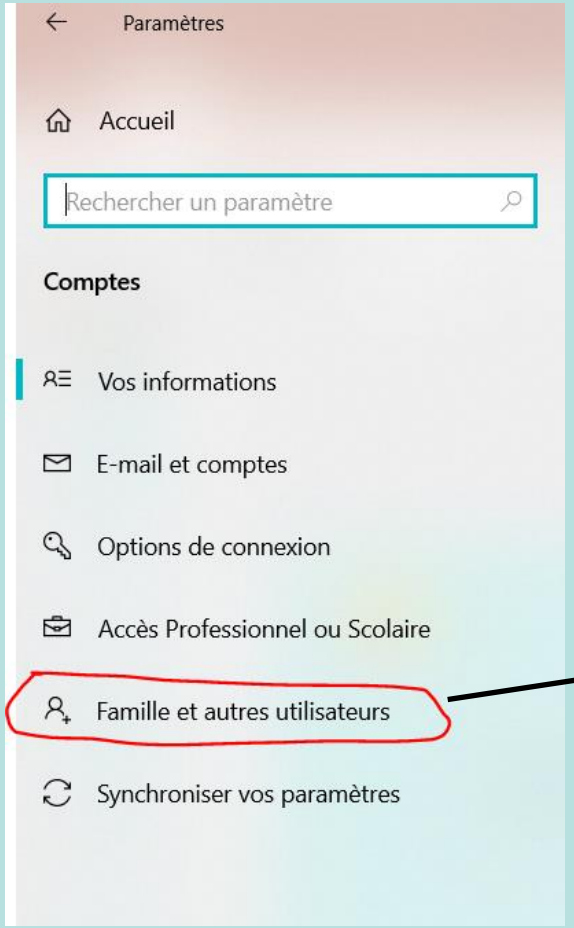


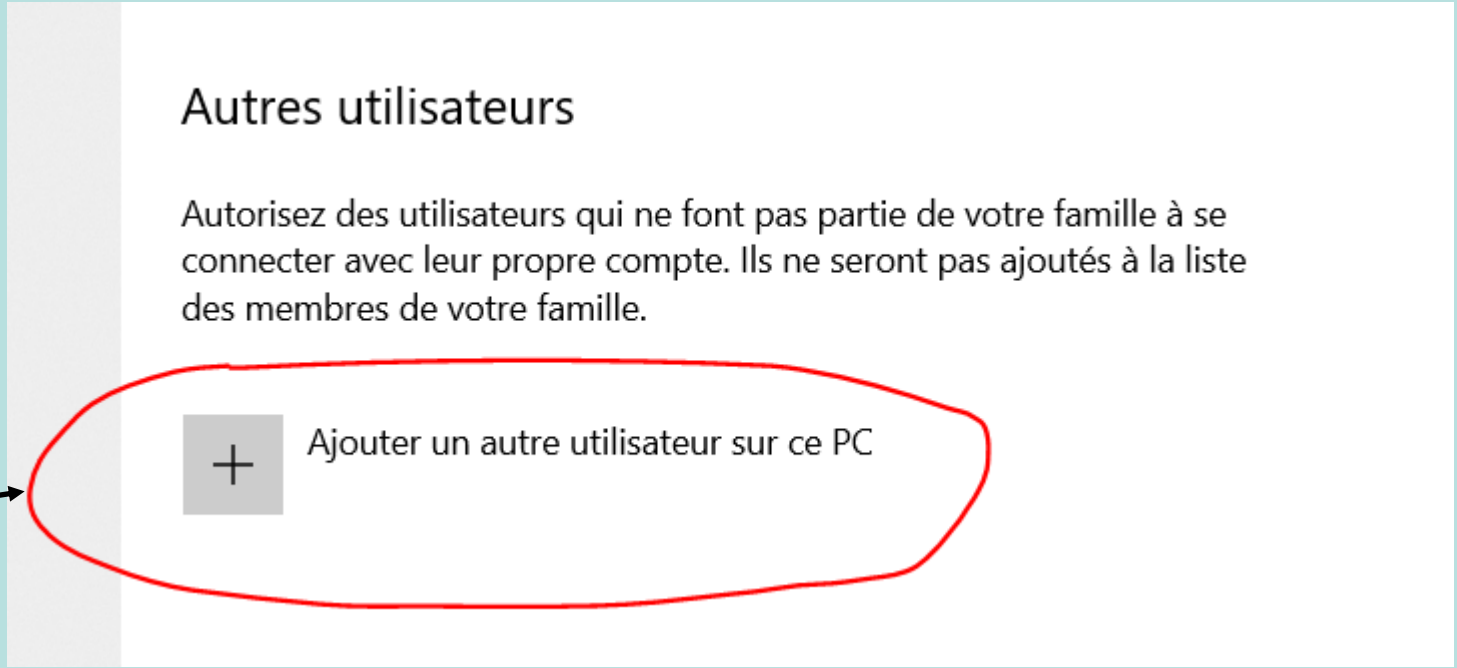
Méthode 2- Ajouter un compte administrateur local

Paramètres / comptes

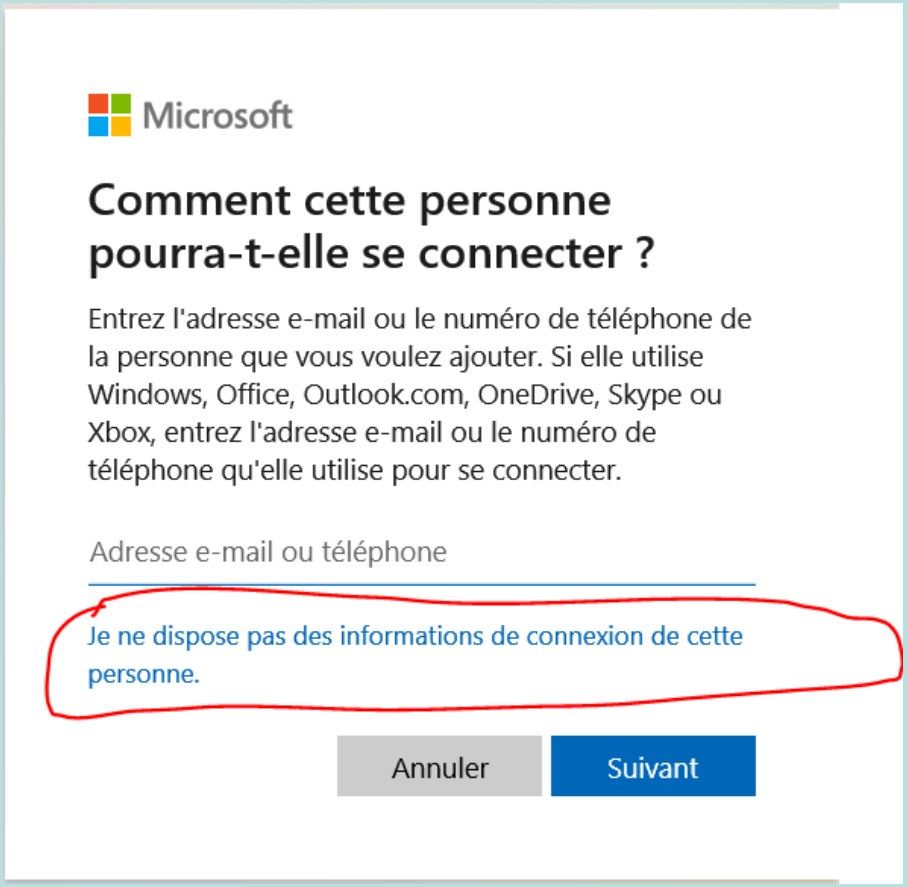


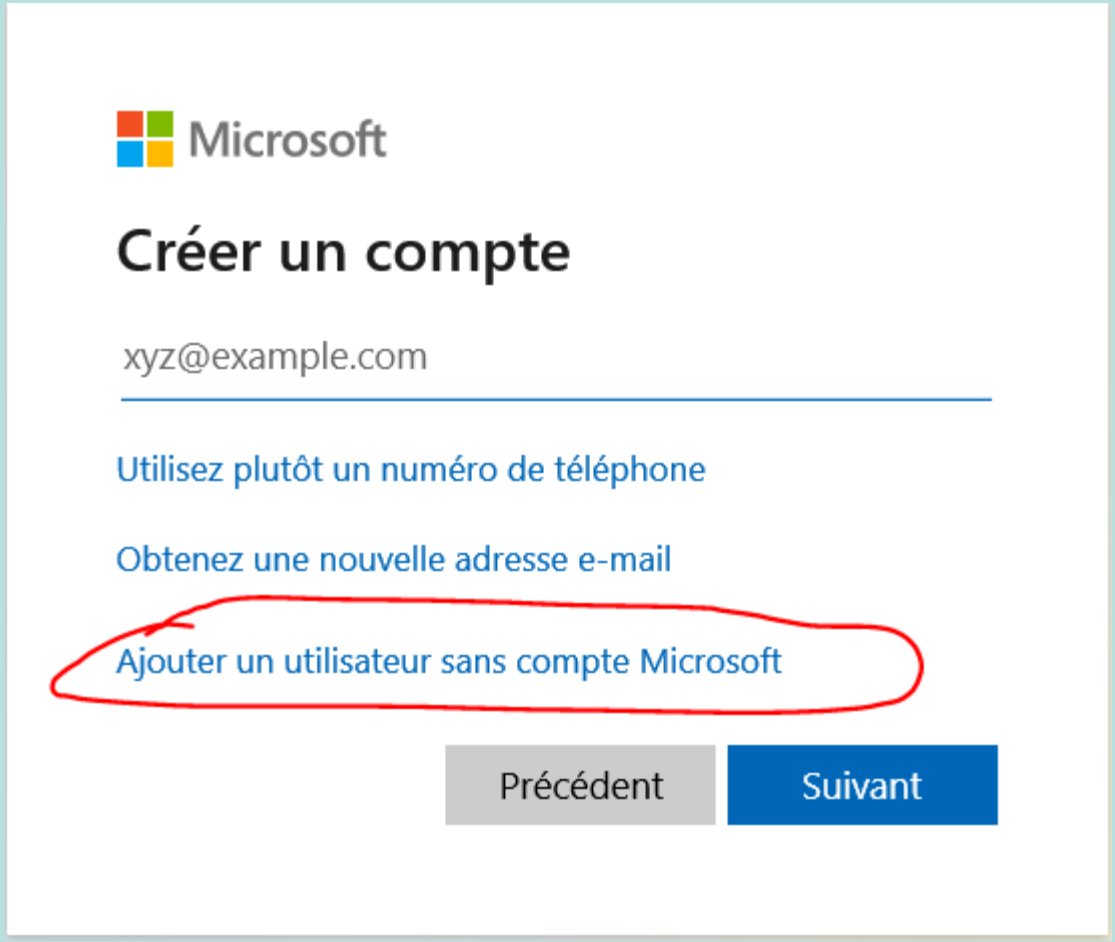
Méthode 2 - Ajouter un compte administrateur local



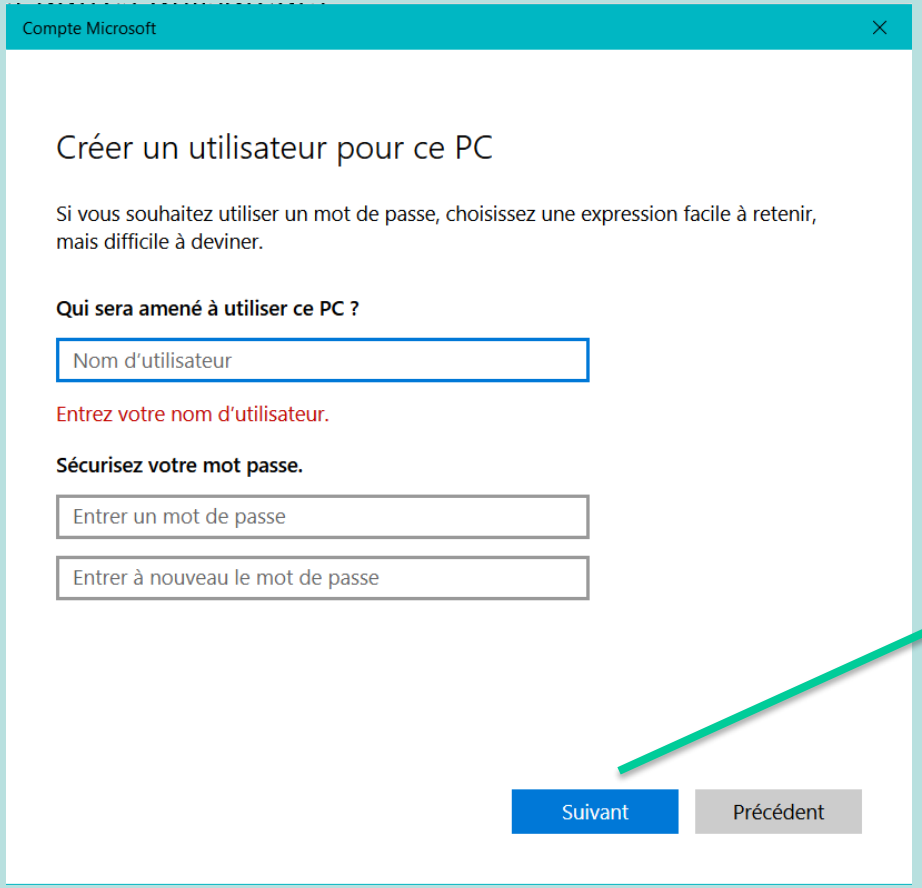


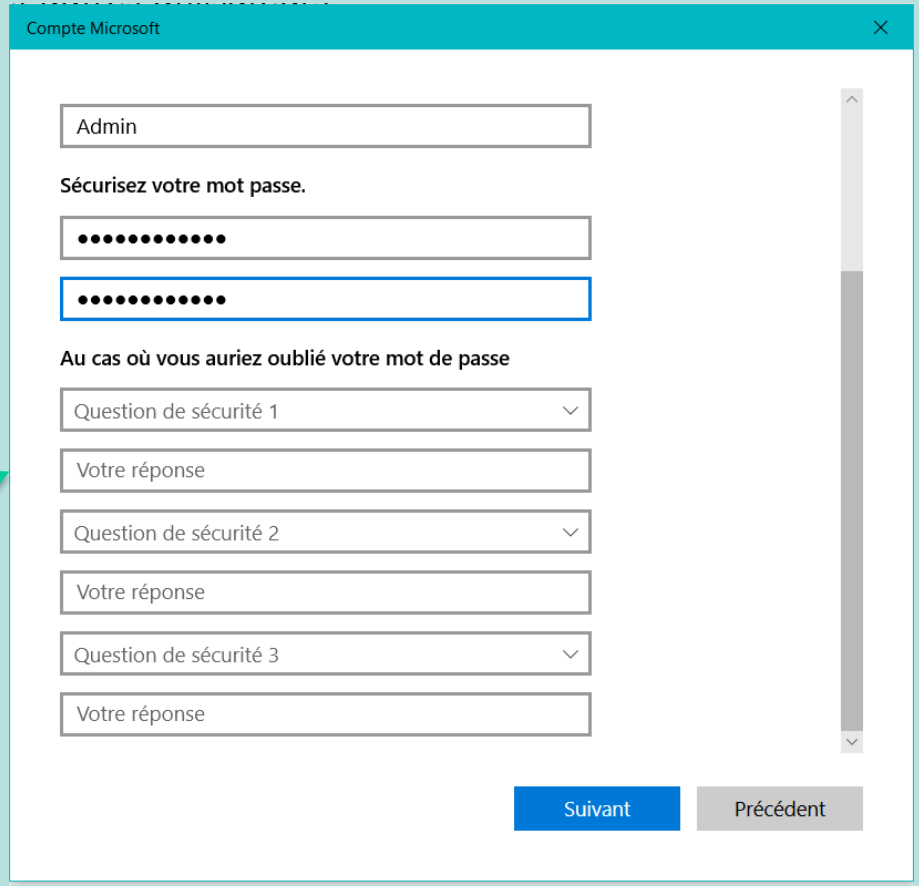
Méthode 2-Ajouter un compte administrateur local



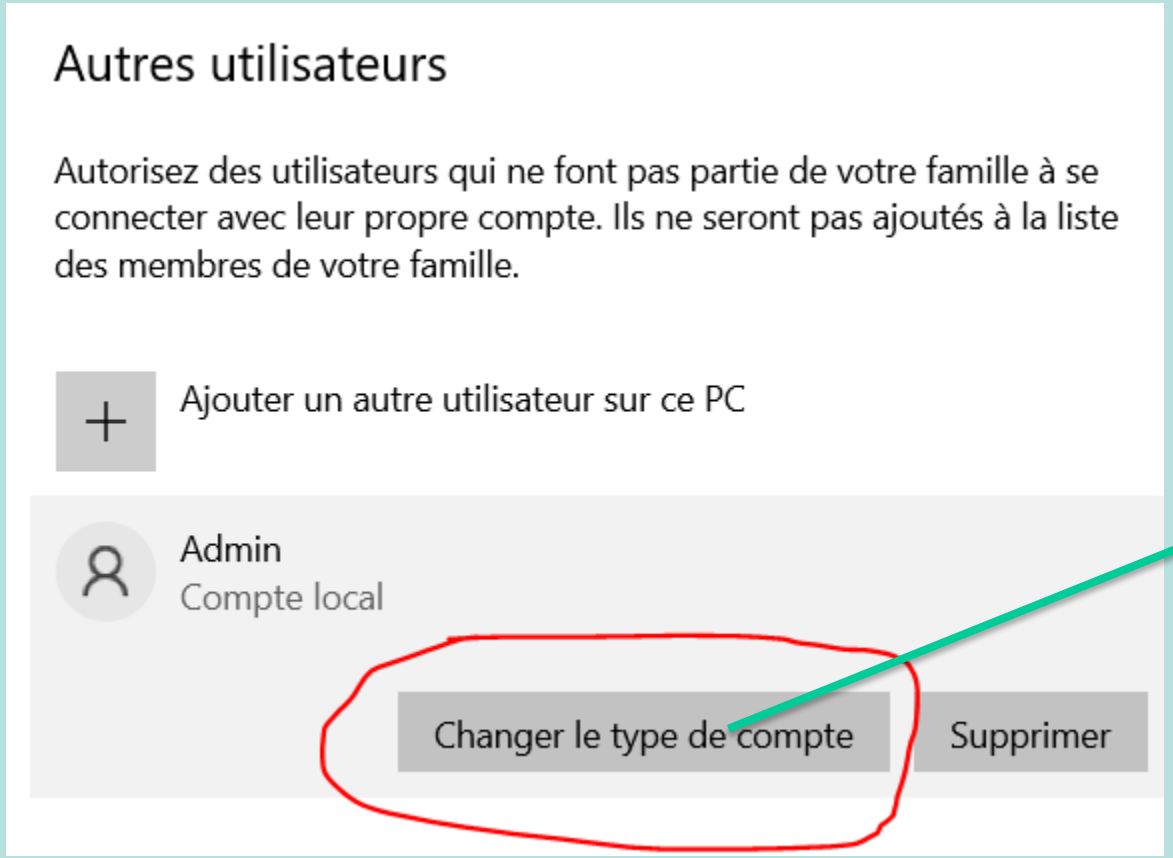


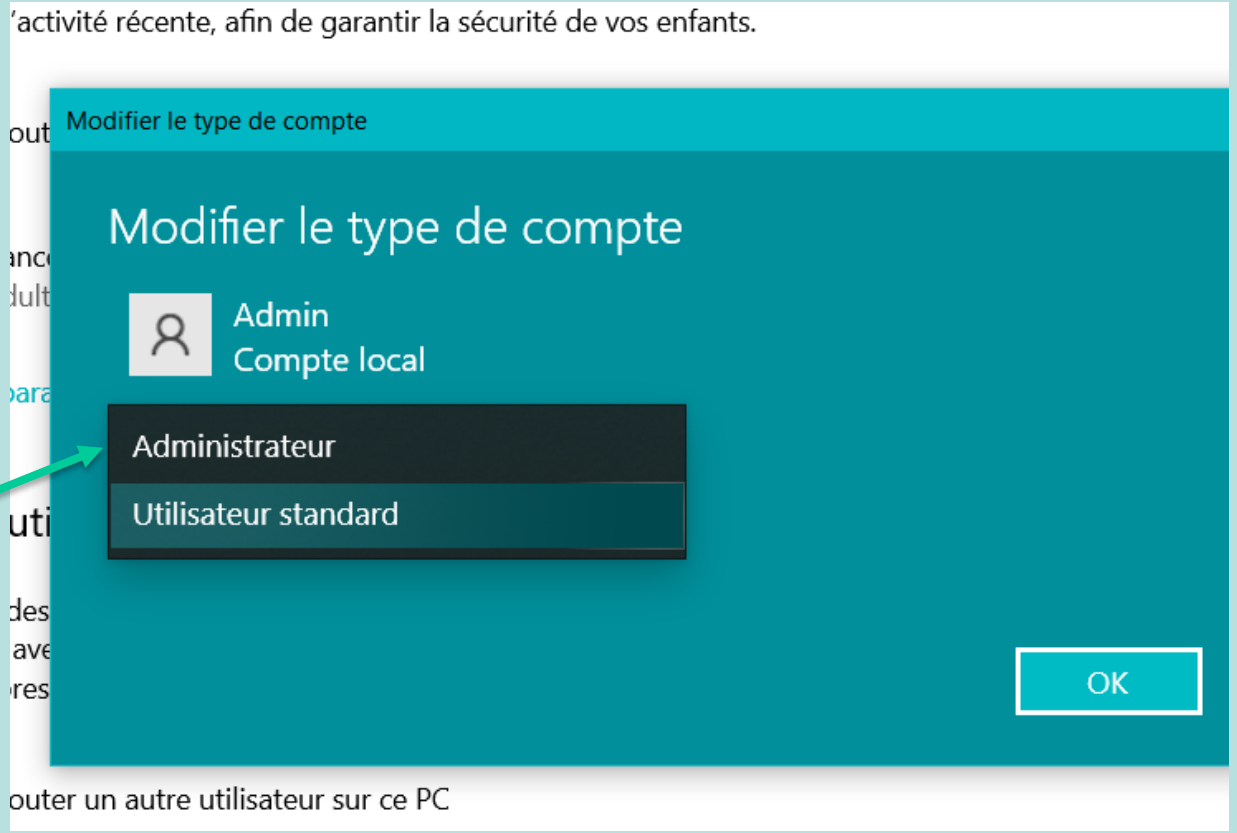
Méthode 2 - Ajouter un compte administrateur local



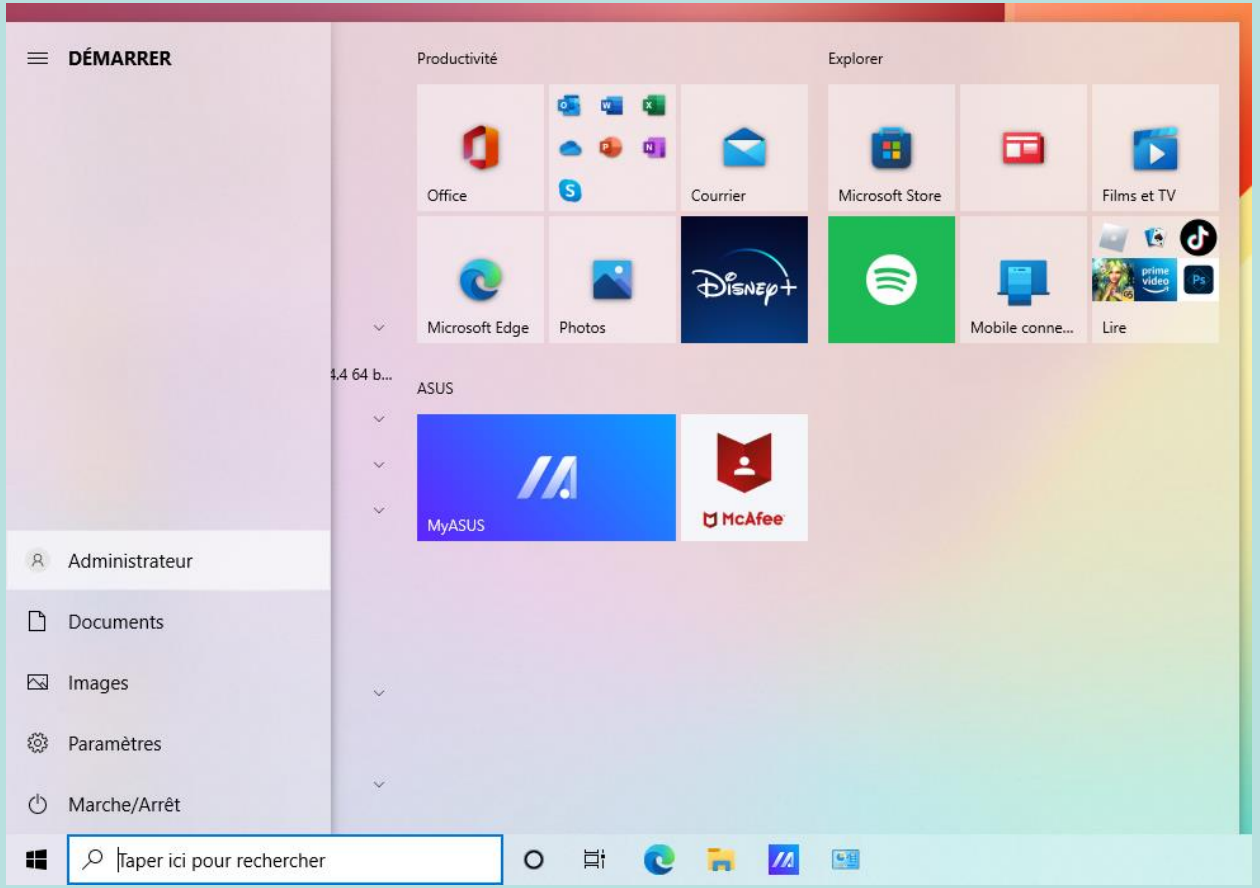


Méthode 2 - Ajouter un compte administrateur local

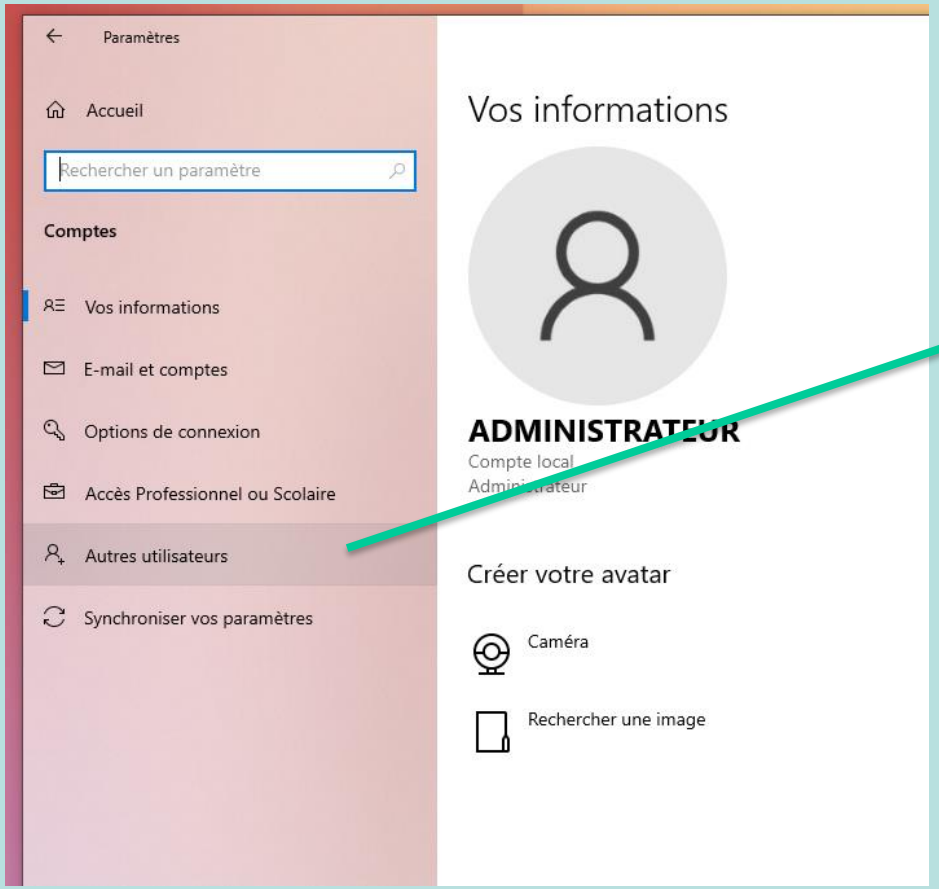


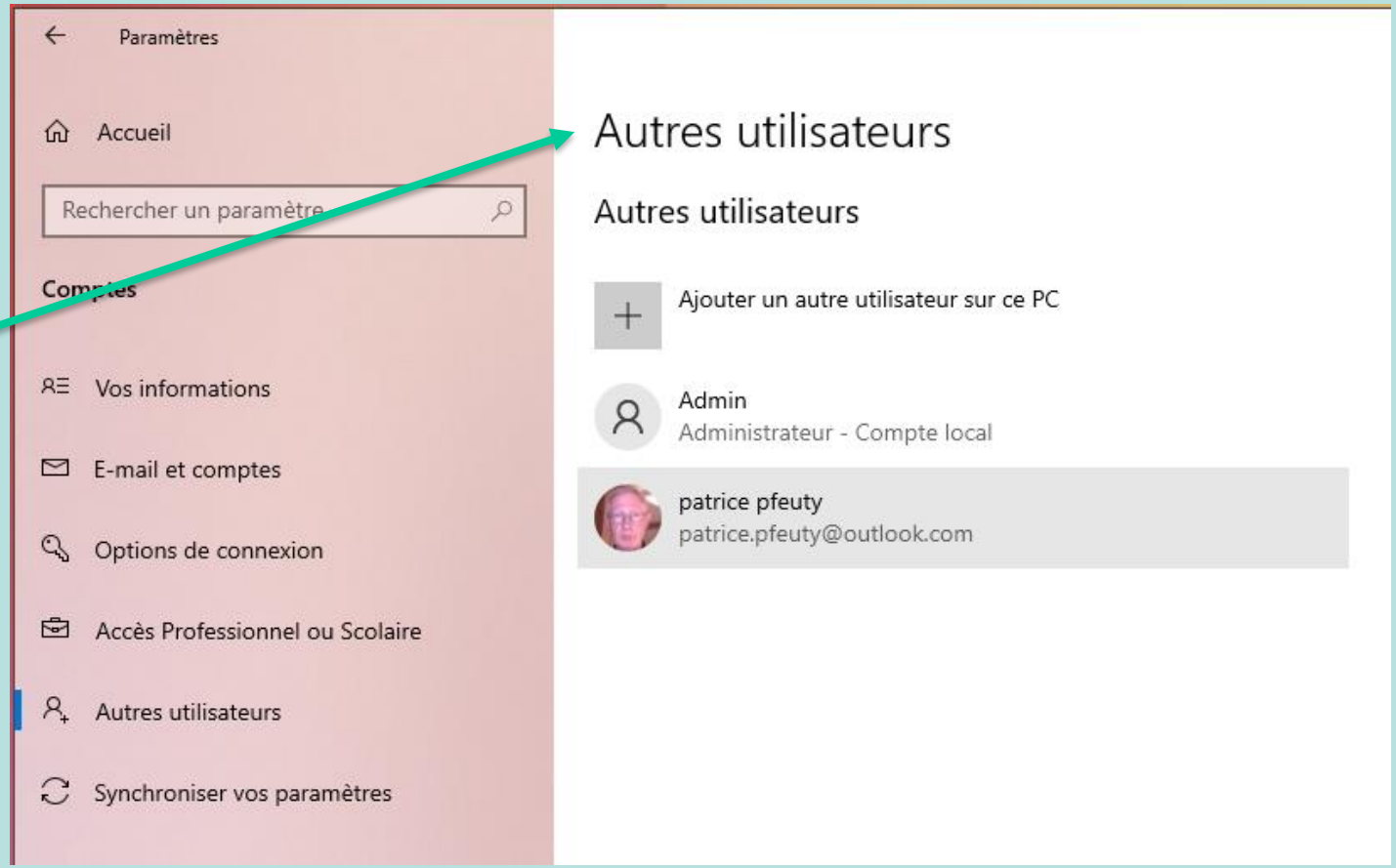


Connexion au compte administrateur

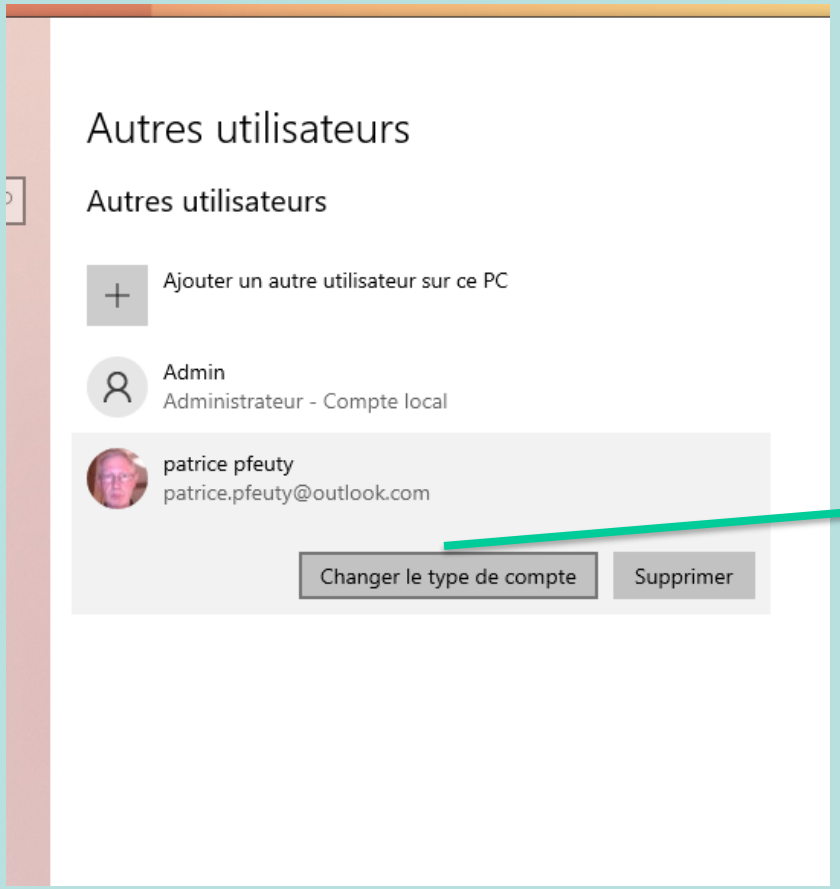


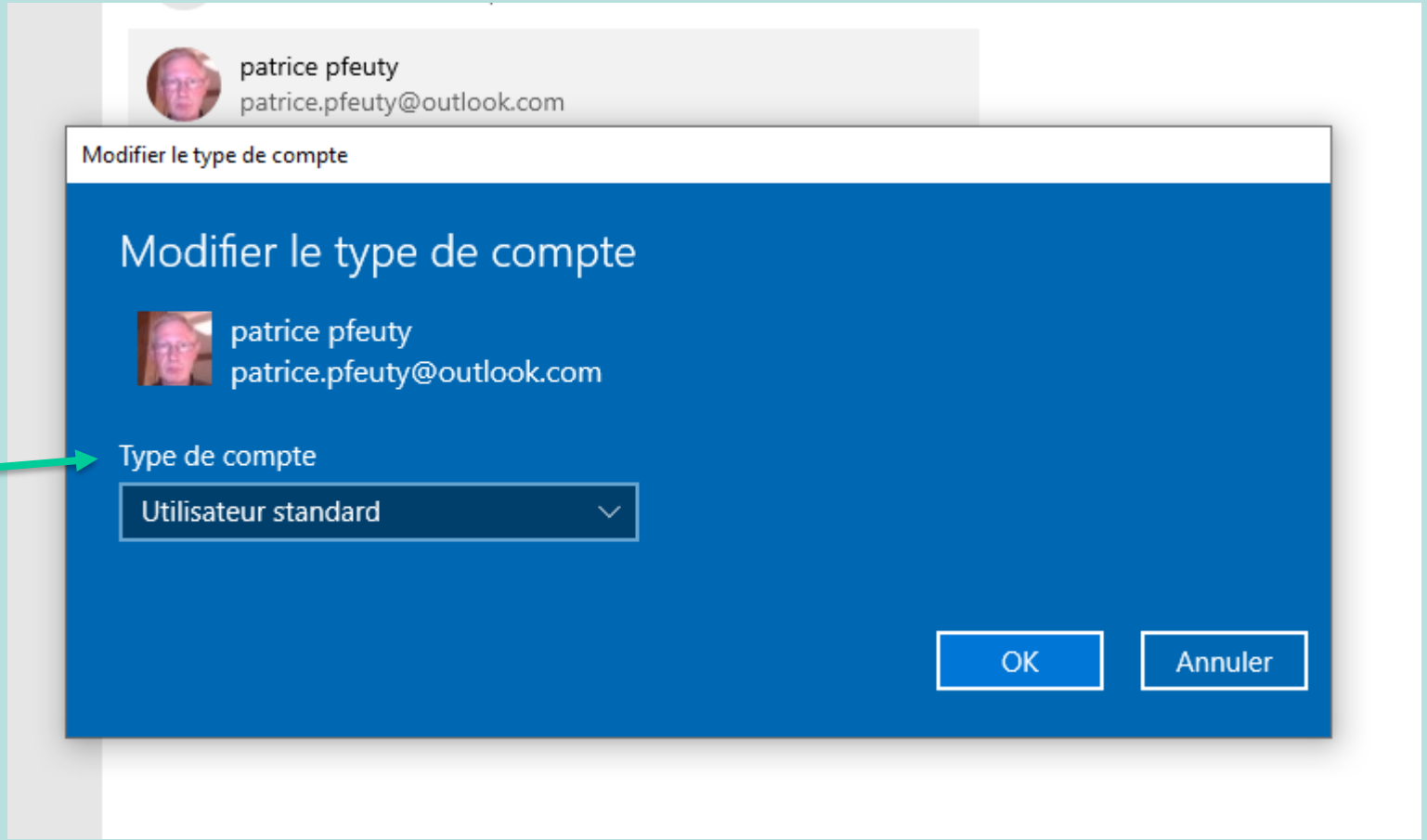
Modification du compte principal





Changer le type de compte du compte principal Windows





Changement du type de compte principal

La modification du type de compte n’est prise en compte qu’après une déconnexion du compte principal et une reconnexion.