



Lundi du numérique du 12 janvier 2026

Cyber sécurité



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 où 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

The screenshot shows the homepage of the 'have i been pwned?' website. The header is dark blue with a navigation menu including 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'Passwords', 'API', 'About', and 'Donate'. The main content area has a blue background with a large white rounded rectangle containing the text 'have i been pwned?'. Below this is a subtitle 'Check if your email or phone is in a data breach'. A search bar with the placeholder 'email or phone (international format)' and a 'pwned?' button is present. A section for 1Password promotion includes the text 'Generate secure, unique passwords for every account' and a link 'Learn more at 1Password.com'. The footer is dark blue and displays statistics: 630 pwned websites, 11,928,699,951 pwned accounts, 115,360 pastes, and 223,156,503 paste accounts.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

630	11,928,699,951	115,360	223,156,503
pwned websites	pwned accounts	pastes	paste accounts



Adresse non compromise

The screenshot shows the 'Have I Been Pwned' website interface. At the top, the logo 'Have I Been Pwned' is displayed in blue. Below it, the text 'Check if your email address is in a data breach' is shown. A search bar contains the email address 'ppfeuty@yahoo.fr', and a blue 'Check' button is to its right. Below the search bar, a link to the 'terms of use' is provided. The section 'Email Breach History' is titled, with the subtitle 'Timeline of data breaches affecting your email address'. A large green box with a red border contains the number '0' and the text 'Data Breaches'. Below this, a message states: 'Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!'.

Have I Been Pwned

Check if your email address is in a data breach

ppfeuty@yahoo.fr **Check**

Using Have I Been Pwned is subject to the [terms of use](#)

Email Breach History

Timeline of data breaches affecting your email address

0
Data Breaches

Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!



Adresse mail compromise

patrice.pfeuty@gmail.com [Check](#)

Using Have I Been Pwned is subject to the [terms of use](#)

Email Breach History

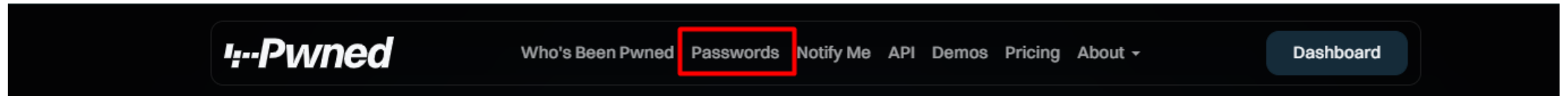
Timeline of data breaches affecting your email address

7
Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.



Verification de mot de passe



Check



Good news — no pwnage found!

This password wasn't found in any of the Pwned Passwords loaded into Have I Been Pwned. That doesn't necessarily mean it's a good password, merely that it's not indexed on this site.



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>



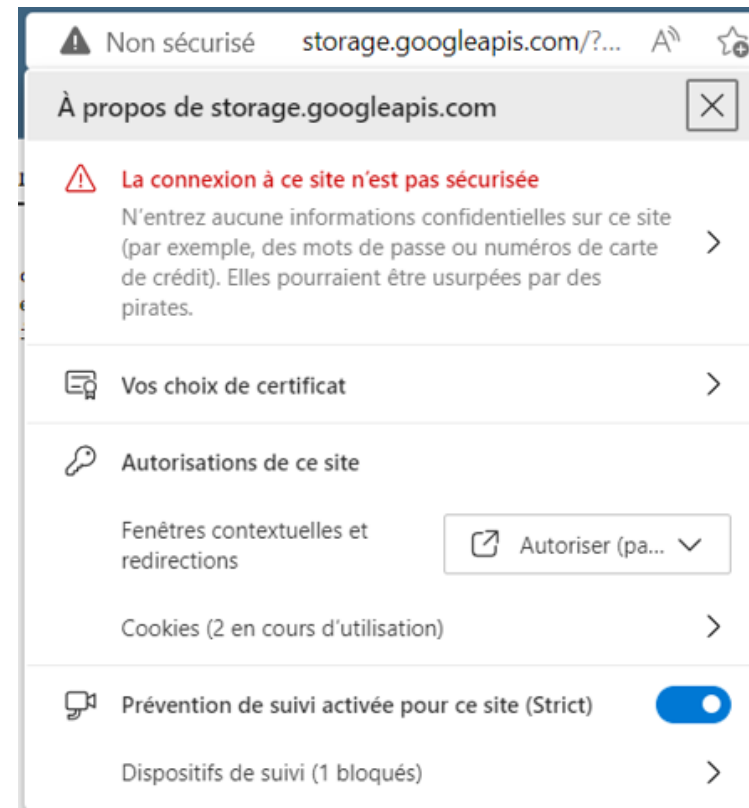
Réputation des sites Internet

- 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 de réputation de sites Web
- [Gridinsoft](#)



Sécurité des sites Internet

- Pour acheter sur Internet, vérifier que le site est sécurisé:
- L'adresse du site doit commencer par **https**





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](#)

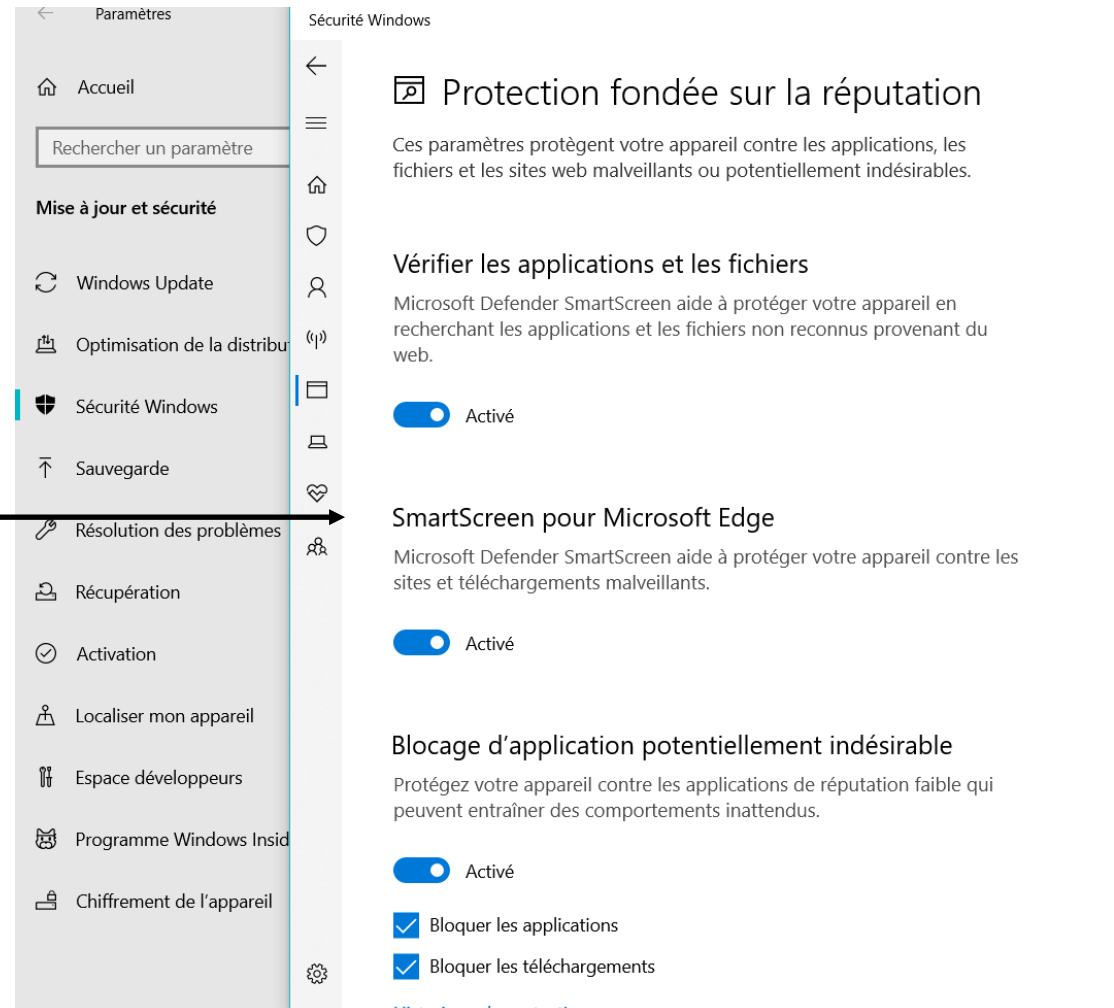
[Ignorer](#)

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.

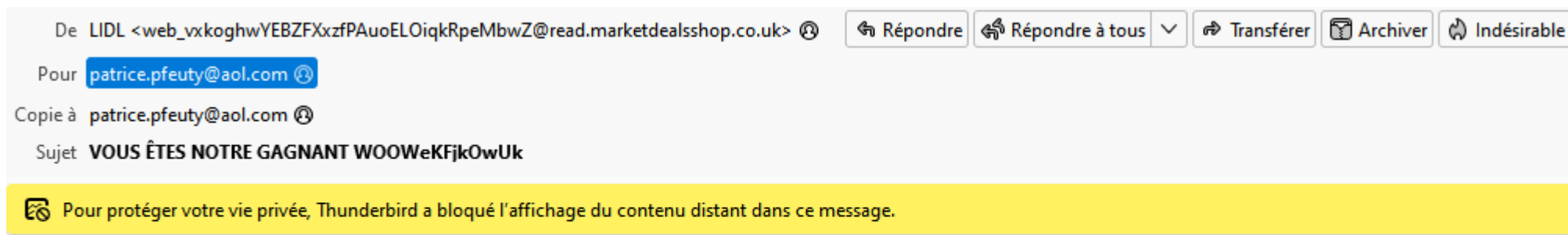
[Paramètres d'Exploit protection](#)

[En savoir plus](#)



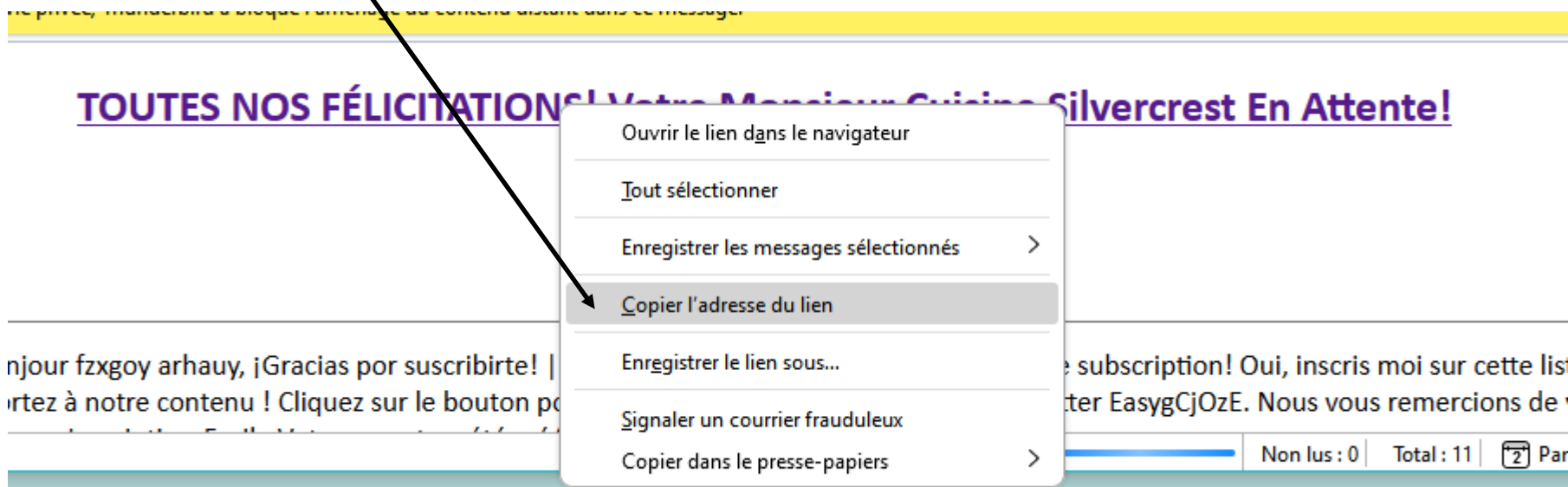


Spam avec risque d'hameçonnage



TOUTES NOS FÉLICITATIONS! Votre Monsieur Cuisine Silvercrest En Attente!

Clic droit

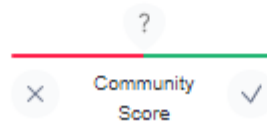




Contrôle d'url avec VIRUSTOTAL



<https://s3-us-west-2.amazonaws.com/12dgfhkuytilkrtjsrahtjd/i.html>



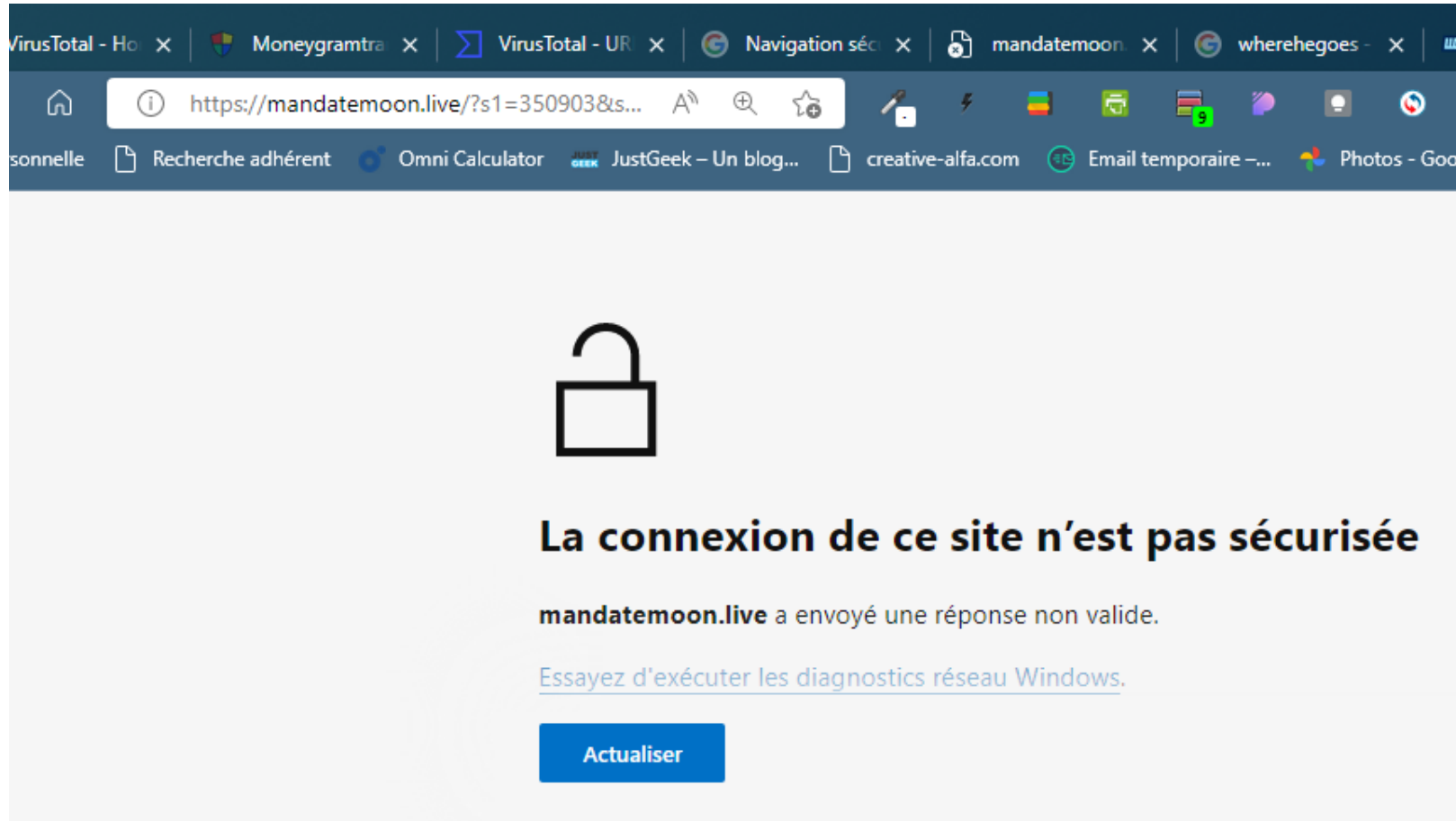
✓ No security vendors flagged this URL as malicious

<https://s3-us-west-2.amazonaws.com/12dgfhkuytilkrtjsrahtjd/i.html>

s3-us-west-2.amazonaws.com



Blocage du site par Edge (SmartScreen)





Contrôle de l'URL avec VIRUSTOTAL

Did you intend to se

 **VIRUSTOTAL**

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH FILES COMMUNITY



https://mandatemoon.live/

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

6 security vendors flagged this URL as malicious

https://mandatemoon.live/
ndatemoon.live

Malicious
Phishing
Malicious
Spam



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

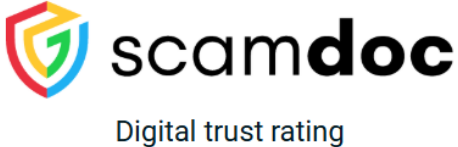
Urgent Contact them now: (moneygramtransferheadoffice80@gmail.com)



Vérification d'adresse mail avec ScamDoc

[Home](#) [Report a scam](#) [Scam Infos](#) [Phone number reliability analysis](#)

   ironman57 ▾



Analysis of the email address "Moneygramtransferheadoffice80@gmail.com"



25%



Trust score

Poor

 You should be wary

Important : If you think the email is linked to a scam on the Internet, you can report it on the Scamwatcher collaborative platform via [the dedicated form](#) .

What do you think of this score?

Leave a comment *