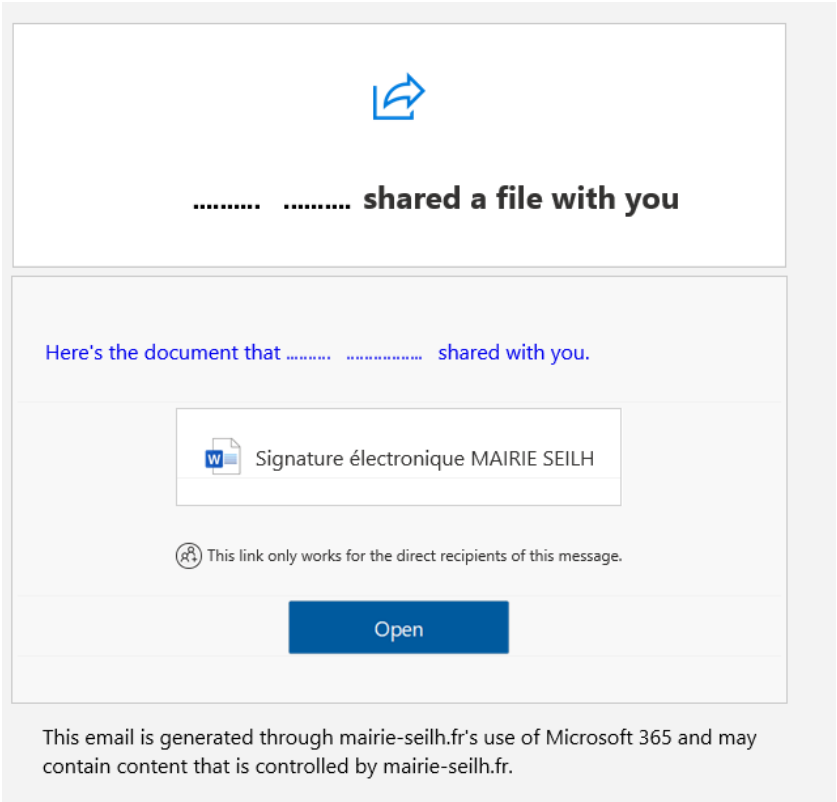
Avis important : tentative d’usurpation par courriel au nom de la mairie

Publié le 23/04/2026

Ce qui s'est passé

La commune de Seilh a été victime d'un acte de cybermalveillance : Une boîte de messagerie de **la mairie de Seilh** a été compromise par un tiers, qui s'en est servi pour diffuser un message frauduleux (tentative d'hameçonnage / phishing) à plusieurs de ses contacts.

Vous avez peut-être reçu ce message frauduleux le 23 avril 2026 avec pour objet « **Re: (prénom) (nom) shared "Signature électronique MAIRIE SEILH" with you** ». Son apparence était légitime puisqu'il provenait réellement de l'adresse de type @mairie-seilh.fr



Ce type d'arnaque s'appelle du **hameçonnage** (ou « phishing » en anglais). Le principe est simple : le pirate envoie un mail qui semble parfaitement légitime — puisqu'il provient réellement de l'adresse de la mairie — pour pousser la personne qui le reçoit à cliquer sur un lien et à saisir ses propres identifiants (adresse mail et mot de passe) sur une fausse page. Une fois ces informations récupérées, le pirate peut à son tour accéder à la boîte mail de la victime, et ainsi de suite.

Dès que nous avons eu connaissance du piratage, nous avons coupé l'accès du pirate, changé le mot de passe, renforcé la sécurité de la boîte et supprimé les paramètres frauduleux qu'il avait installés. L'incident a été signalé à la CNIL et une plainte a été déposée.

Avez-vous reçu ce mail ?

Si vous avez reçu ce mail mais n'avez rien fait

Vous pouvez simplement le supprimer. Par précaution, restez vigilant sur les mails reçus récemment depuis l'adresse de la mairie : en cas de doute sur un message, appelez-nous directement au 05 61 59 90 13 avant de cliquer sur quoi que ce soit.

Si vous avez cliqué sur le lien et saisi votre adresse mail et votre mot de passe

Il est probable que votre propre boîte mail soit maintenant accessible au pirate. Voici, pas à pas, ce qu'il faut faire **dans l'ordre et sans attendre**.

1. Changez immédiatement votre mot de passe

Rendez-vous sur le site de votre messagerie (Gmail, Orange, Outlook, Yahoo, Free, etc.) et changez votre mot de passe. Choisissez un mot de passe long (au moins 12 caractères), mélangeant lettres, chiffres et symboles, et **que vous n'utilisez sur aucun autre site**. Si vous utilisiez le même mot de passe sur d'autres comptes (réseaux sociaux, achats en ligne, impôts…), changez-le également partout — c'est le premier réflexe du pirate que d'essayer ce mot de passe ailleurs.

2. Activez la « double authentification »

C'est la mesure la plus efficace. Derrière ce nom technique se cache un principe simple : en plus du mot de passe, votre messagerie vous demandera une seconde preuve pour se connecter — généralement un code reçu par SMS ou une validation dans une application sur votre téléphone. Même si un pirate connaît votre mot de passe, il ne pourra pas entrer sans votre téléphone. Cette option s'active dans les **paramètres de sécurité** de votre messagerie (cherchez « double authentification », « validation en deux étapes » ou « 2FA »).

3. Vérifiez que le pirate n'a pas installé de « pièges » dans votre boîte

C'est le point le plus important et le plus souvent oublié. Lorsqu'un pirate accède à une boîte mail, il installe généralement des règles automatiques invisibles, qui lui permettent de continuer à espionner vos mails **même après que vous avez changé votre mot de passe**. Il faut donc les chercher et les supprimer.

Dans les paramètres de votre messagerie, regardez :

- les **règles de transfert automatique** : vérifiez qu'aucun transfert n'est activé vers une adresse que vous ne connaissez pas. Si vous en trouvez un, supprimez-le.
- les **règles de filtrage ou de tri automatique** : le pirate peut avoir créé une règle qui déplace directement à la corbeille certains mails (par exemple ceux contenant les mots « sécurité », « banque » ou « mot de passe »), pour que vous ne voyiez pas les alertes.
- la **signature** et la **réponse automatique** : vérifiez qu'elles n'ont pas été modifiées.

Si vous ne savez pas où trouver ces paramètres, la plupart des messageries proposent une page d'aide « mon compte a été piraté » qui guide pas à pas. Les principaux fournisseurs (Gmail, Outlook, Orange, Yahoo, Free) disposent également d'une procédure dédiée accessible depuis leur page d'aide.

4. Vérifiez les connexions récentes

La plupart des messageries permettent de voir depuis quels appareils et quels lieux votre boîte a été consultée récemment. Si vous voyez une connexion que vous ne reconnaissez pas (un autre pays, un appareil inconnu), déconnectez toutes les sessions — il y a généralement un bouton « se déconnecter de tous les appareils ».

5. Prévenez vos contacts

Si votre boîte a été utilisée pour envoyer à son tour des mails frauduleux, prévenez vos proches et collègues pour qu'ils ne cliquent sur rien. Un simple message ou un appel suffit.

6. Si vous avez subi un préjudice financier ou une utilisation frauduleuse

Déposez plainte. Vous pouvez le faire :

- en ligne sur **17Cyber.gouv.fr**, le service officiel d'assistance aux victimes de cybermalveillance, disponible 24h/24 ;
- ou directement au commissariat ou à la gendarmerie la plus proche.

Le site **cybermalveillance.gouv.fr** propose également une assistance gratuite et des fiches pratiques.

Comment reconnaître un mail frauduleux à l'avenir

Quelques réflexes simples permettent de repérer la plupart des tentatives de phishing :

Un mail qui crée un **sentiment d'urgence** (« votre compte va être fermé », « dernière chance », « réponse sous 24 h ») doit éveiller la méfiance — c'est un ressort classique des arnaques. De même, un mail qui vous demande de **cliquer pour saisir vos identifiants**, de **confirmer vos coordonnées bancaires** ou de **télécharger un document inattendu** mérite vérification, même s'il semble venir d'un expéditeur connu : avant de cliquer, posez le pointeur de votre souris (sans cliquer) sur le lien, l'adresse réelle s'affiche en bas de l'écran — si elle ne correspond pas au site officiel annoncé, c'est une arnaque.

En cas de doute sur un mail apparemment envoyé par la mairie, **ne répondez pas au mail, n'utilisez pas les numéros qui y figurent**, mais appelez-nous directement au **05 61 59 90 13** ou venez nous voir à l'accueil.

Nous contacter

Pour toute question sur cet incident, vous pouvez joindre :

- **La mairie :** 05 61 59 90 13 — accueil@mairie-seilh.fr
- **Le Délégué à la protection des données (DPO) :** rgpd@mairie-seilh.fr

Nous vous présentons nos excuses pour la gêne occasionnée et vous remercions de votre vigilance.