

PIRATAGE DE MESSAGERIE ÉLECTRONIQUE

IDENTIFICATION ET PREMIÈRES ACTIONS À MENER

[À DIFFUSER LARGEMENT À TOUS LES COLLABORATEURS]












1

Le piratage d'une messagerie électronique fait référence à une prise de contrôle de votre messagerie par **un tiers malveillant**. Ce tiers peut librement consulter notamment vos e-mails, vos carnets d'adresses voire vos espaces de stockage cloud afin de :

- Subtiliser des informations personnelles, professionnelles et/ou bancaires,
- Se faire passer pour vous notamment auprès de vos partenaires (ex : pour se faire livrer du matériel en votre nom),
- Mettre en place une future «fraude au Président»...



Suis-je victime d'un piratage de ma messagerie électronique ?

Identification du piratage	Personne concernée pour détecter le piratage	Risques	Actions réalisées (à compléter par l'utilisateur)	
			OUI	NON
Vous n'arrivez plus à vous connecter à votre compte e-mail avec vos identifiants.	Seul			
Vous trouvez, dans vos messages envoyés, des e-mails dont vous n'êtes pas l'auteur.	Seul			
Vous recevez des messages dont vous ne comprenez pas la nature et venant d'un auteur que vous connaissez.	Seul			
Vous recevez une réponse à un message que vous n'avez pas envoyé.	Seul			
Sans demande de votre part, vous recevez des messages de demande de changement de mots de passe ou de mots de passe oubliés (peut provenir de n'importe quel service en ligne).	Seul			
Vous recevez des e-mails de personnes qui affirment avoir reçu des e-mails de votre part dont vous n'êtes pas l'auteur.	Seul			
Vous recevez une notification qui vous indique une tentative de connexion à votre compte à partir d'un appareil, d'une localisation ou d'une adresse IP que vous ne connaissez pas.	Service IT			
Vous constatez la présence d'un appareil que vous ne connaissez pas dans votre historique de connexions.	Service IT			
Vous identifiez que des informations personnelles (nom, prénom, date de naissance, numéro de téléphone...) ou des paramètres de votre compte ont été modifiés.	Service IT			
Vous découvrez que des règles de filtrage ou de redirection de vos messages ont été mises en place à votre insu.	Service IT			
Vous vous apercevez que des contacts ont été ajoutés ou modifiés de votre compte sans votre accord.	Service IT			

Légende



Alerte forte



Alerte moyenne



1 ou + alarme(s) forte(s) : réagir immédiatement



1 alarme moyenne : être prudent



2 alarmes moyennes : réagir immédiatement

PIRATAGE DE MESSAGERIE ÉLECTRONIQUE IDENTIFICATION ET PREMIÈRES ACTIONS [À DIFFUSER LARGEMENT À TOUS LES COLLABORATEURS]

1

Comment réagir ?

- **Immédiatement**, prévenir le service informatique ou le prestataire informatique de son entreprise,
- Vous pouvez vous faire accompagner en cliquant sur le site internet : cybermalveillance.gouv.fr,
- Se référer aux règles de bonnes pratiques et de sécurité de l'entreprise.

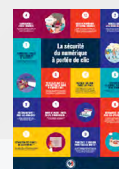
Les actions à mener seul ou avec votre service informatique	Actions réalisées (à compléter par l'utilisateur)	
	OUI	NON
1. Démarche auprès des autorités compétentes à réaliser dans les 72h à partir du moment où vous avez eu connaissance de la compromission		
Déposer plainte au plus tard dans les 72h.		
La preuve du dépôt de plainte devra être présentée à votre courtier ou à votre assureur.		
Notifier à la CNIL la supposée violation de données personnelles dans les 72h.		
2. Gestion de mot de passe		
Procéder à un changement de mot de passe de son compte de messagerie ainsi que sur tous les autres sites où vous utilisez le même mot de passe.		
Mettre en place une authentification renforcée.		
Stocker son mot de passe dans un coffre-fort (cf. rubrique « coffre-fort » du guide ANSSI).		
3. Autres actions		
Vérifier l'absence de règle de filtrage ou de redirection de vos messages.		
Prévenir les contacts de votre compte de messagerie.		
Demander aux collègues de réaliser les mêmes actions.		
Alerter votre banque et surveiller vos comptes bancaires.		
Effectuer une analyse complète de votre poste de travail avec antivirus.		

Rester vigilant quelques temps, revoir cette check-list périodiquement

Pour aller plus loin



Vérifier sur le site <https://haveibeenpwned.com> quelles autres informations auraient pu m'être dérobées



Former vos équipes

Des posters sont disponibles sur les sites suivants : ANSSI - CNIL - cybermalveillance.com

Contacts en cas d'urgence

- **Cybermalveillance.fr** : contact@cybermalveillance.gouv.fr
- **CNIL** (Commission Nationale de l'Informatique et des Libertés) : 01.53.73.22.22
- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) : 01.71.75.84.68 // cert-fr.cossi@ssi.gouv.fr
- **Assureur du risque cyber**