

6 QUESTIONS À SE POSER

POUR RECONNAITRE UN EMAIL MALVEILLANT

Qu'est-ce que le phishing ?

Le phishing (ou *hameçonnage*) est une technique de fraude utilisée par des cybercriminels qui consiste à se faire passer pour une organisation ou une personne légitime afin d'inciter la victime à divulguer des informations sensibles ou à effectuer une action risquée (cliquer sur un lien, ouvrir une pièce jointe).

1. Contexte	Est-ce légitime que je reçoive cet email ?	<ul style="list-style-type: none">Le sujet du message correspond-il à mon activité ou à mes responsabilités ?Ai-je récemment effectué une action qui expliquerait la réception de cet email (commande, inscription, support) ?
2. Ton	Le ton du message semble-t-il habituel ?	<ul style="list-style-type: none">Le message cherche-t-il à me faire agir rapidement en évoquant une urgence, un problème, une sanction ou un gain ?Le contenu du message est-il inhabituel, trop bref ou peu professionnel ?
3. Expéditeur	L'expéditeur est-il bien celui qu'il prétend être ?	<ul style="list-style-type: none">Est-ce que j'ai déjà interagi avec cette personne ou cette entité ?L'adresse email est-elle correctement écrite et non légèrement modifiée (inversion de lettres par exemple) ?
4. Lien suspect	Le message me demande-t-il de cliquer sur un lien ?	<ul style="list-style-type: none">En survolant le lien (sans cliquer), est-ce que l'adresse affichée correspond à un site connu et non une adresse étrange ?Après avoir cliqué, suis-je redirigé vers une page inattendue, notamment une page de connexion ou de saisie d'informations ?
5. Actions à risque	Y a-t-il des pièces jointes ou des actions à risque ?	<ul style="list-style-type: none">L'email me pousse-t-il à transmettre des informations sensibles (identifiants, code reçu par SMS, coordonnées bancaires, etc.) ?Est-ce qu'on me demande d'installer quelque chose sur mon ordinateur ou de télécharger une pièce jointe ?
6. Réaction	Que faire avec cet email ?	<ul style="list-style-type: none">Dans ce cas, ne cliquez pas et ne répondez pas.Si nécessaire, contactez l'expéditeur par un canal officiel et indépendant de l'email, puis transférez le message à votre support informatique (si applicable).

[Alerte sécurité] Activité inhabituelle détectée



Service sécurité <service.sécurité@vauud.ch>

À [redacted]

Bonjour,

Suite à une activité inhabituelle, **vos accès seront suspendus dans les prochaines 24 heures** si aucune vérification n'est effectuée.

Afin d'éviter toute interruption, merci de confirmer immédiatement vos informations.

Confirmer vos accès:

[Alerte sécurité à vérifier](#)

<https://bit.ly/Alerte-sécurité>

Cliquez en maintenant le bouton Ctrl enfoncé pour suivre le lien

Nous vous remercions de votre compréhension.

Service sécurité
021 346 43 98

Ne pas répondre à ce message

Exemple d'email malicieux