

## QUE FAIRE SI VOUS AVEZ RÉPONDU À UN EMAIL DE PHISHING ?

---

Les attaques de phishing sont de plus en plus fréquentes et sophistiquées. Les cybercriminels développent constamment de nouvelles techniques pour inciter les utilisateurs à divulguer des informations sensibles. Que les pirates utilisent des emails, des messages sur les réseaux sociaux ou des appels téléphoniques frauduleux dans leurs campagnes, les escroqueries de phishing réussies peuvent avoir de graves conséquences en termes de pertes financières et d'atteinte à la réputation.

### Types d'attaques de phishing

Les attaques de phishing peuvent prendre de nombreuses formes. Mais elles ont toutes un objectif commun : inciter les utilisateurs à divulguer des informations sensibles, comme des identifiants de connexion, des informations de compte ou des fichiers et des données.

**COMPRENDRE LES DIFFÉRENTS TYPES D'ATTAQUES DE PHISHING COURANTES PEUT VOUS AIDER À LES DÉTECTER :**

1. **Phishing par email.** Il s'agit du type d'attaque de phishing le plus répandu. Un cybercriminel envoie un email semblant provenir d'une source de confiance, telle qu'une banque ou une entreprise de renom. Il est donc important de bien vérifier l'adresse e-mail de l'expéditeur ; Les e-mails de phishing cherchent souvent à créer un sentiment d'urgence pour inciter à agir rapidement ; le mail contient des liens suspects, des demandes d'informations sensibles ; contiennent des fautes de grammaire ou d'orthographe.
2. **Spear phishing.** Il s'agit d'une forme d'attaque de phishing plus ciblée. Dans une attaque de spear phishing (harponnage), le cybercriminel fait des recherches sur les centres d'intérêt et les informations personnelles de la victime pour créer un email de phishing plus convaincant et personnalisé. Ce type d'attaque est souvent utilisé pour cibler des cadres dirigeants ou des personnalités de premier plan.
3. **Vishing.** Dans une attaque de vishing (phishing vocal), le cybercriminel appelle la victime et se fait passer pour un représentant d'une entreprise de confiance, comme une banque ou un organisme public. Le cyberpirate peut employer des techniques d'ingénierie sociale pour inciter la victime à divulguer des informations sensibles par téléphone.
4. **SMiShing.** Contrairement au vishing, dans une attaque de SMiShing, le cybercriminel ne passe pas un appel téléphonique, mais envoie un SMS. Le message peut contenir un lien qui dirige la victime vers un site Web frauduleux, ou demander à celle-ci de divulguer des informations sensibles.

### MESURES À PRENDRE SI VOUS RÉPONDEZ À UN EMAIL DE PHISHING

Si vous pensez avoir répondu à un email de phishing, vous devez agir rapidement pour limiter les dégâts. Voici quelques étapes à suivre :

1. **Modifiez vos mots de passe.** Commencez par modifier *immédiatement* vos mots de passe. Vous devriez modifier régulièrement vos mots de passe. Ils doivent être complexes, uniques

et difficiles à deviner. Évitez d'utiliser le même mot de passe pour plusieurs comptes. Ne communiquez vos mots de passe à personne.

2. **Informez** dans les plus brefs délais votre fournisseur de messagerie de la réception de l'email de phishing.
3. **Signalez aux autorités compétentes.** En France, vous pouvez le transmettre à l'adresse [phishing-initiative@ssi.gouv.fr](mailto:phishing-initiative@ssi.gouv.fr), qui est gérée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette démarche aide à collecter et analyser les e-mails frauduleux afin de mettre en place des mesures pour bloquer les attaques futures.
4. **Surveillez vos comptes.** Si vous avez répondu à un email de phishing, vous devez impérativement procéder à une analyse antimalware. Les malwares sont des logiciels malveillants conçus pour endommager ou désactiver les systèmes informatiques, subtiliser des informations sensibles ou espionner les activités des utilisateurs. Les cybercriminels utilisent souvent des emails de phishing pour distribuer des malwares. C'est pourquoi il est essentiel d'analyser votre terminal à la recherche de virus ou d'autres logiciels malveillants.
5. **Contactez l'entreprise ou l'organisme.** Si vous avez répondu à un email de phishing semblant provenir d'une source de confiance, contactez l'entreprise ou l'organisme concerné pour l'avertir. Il pourra peut-être prendre des mesures pour éviter que d'autres clients ou collaborateurs soient victimes de la même escroquerie.

#### **QUE FAIRE EN CAS DE MAIL SUSPECT ?**

1. Ne pas cliquer sur les liens : Ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes.
2. Vérifier avec l'émetteur : Contactez directement l'entreprise ou la personne qui aurait envoyé le message pour confirmer sa légitimité.
3. Signaler l'e-mail : Informez votre service informatique ou le responsable de la sécurité des informations.
4. Supprimer le message : Après avoir pris les mesures nécessaires, supprimez le message.

Sources : [cyber-securite.fr/proofpoint.com](https://cyber-securite.fr/proofpoint.com)