# 10 façons de prévenir les attaques de phishing

Table des matières



**Connaissez-vous les dangers des attaques de phishing ?** Selon un récent rapport de Verizon, 82 % des cyberattaques sont dues à un facteur humain : vol d'informations d'identification, attaques de phishing, ingénierie sociale, usurpation d'identité, utilisation abusive ou erreur.

## Qu'est-ce qu'une attaque de phishing ?

Le phishing est une cyberattaque au cours de laquelle les attaquants se font passer pour des entités légitimes afin d'inciter à divulguer des informations sensibles. Ces attaques se présentent souvent sous la forme d'e-mails, de SMS ou d'appels téléphoniques qui semblent provenir de sources fiables, telles que des banques, des entreprises ou des collègues. L'objectif principal du phishing est d'inciter les destinataires à révéler des informations personnelles telles que leur nom d'utilisateur, leur mot de passe ou leur numéro de carte bancaire.

## Principales techniques de phishing

Les attaques de phishing peuvent varier considérablement dans leur approche, mais les techniques les plus courantes sont les suivantes :

- **Spear Phishing** : attaques ciblées visant des personnes ou des organisations en particulier, utilisant souvent des informations personnalisées pour paraître plus convaincantes.
- **Phishing par clonage** : un e-mail légitime contenant une pièce jointe ou un lien est copié et renvoyé, mais le contenu d'origine est modifié de manière malveillante.
- **Whaling** : attaques de phishing très médiatisées ciblant des cadres supérieurs ou des personnalités importantes au sein d'une entreprise, impliquant souvent des messages hautement personnalisés et persuasifs.
- **Smishing** : tentatives de phishing par SMS, au cours desquelles les attaquants envoient des messages contenant des liens ou des demandes d'informations personnelles.

## Pourquoi le phishing est-il une source de préoccupation majeure pour les particuliers et les entreprises ?

Le phishing est une source de préoccupation majeure car il peut causer des dommages importants. Pour les particuliers, être victime d'un hameçonnage peut entraîner des pertes financières, une usurpation d'identité et des fuites de données personnelles. Pour les entreprises, les attaques de phishing peuvent entraîner la compromission d'informations sensibles, des pertes financières, une atteinte à la réputation et des perturbations opérationnelles.

## 10 Conseils pour Éviter les Attaques de Phishing

### 1 - Éduquez-vous

Restez informé des dernières tactiques d'hameçonnage en participant à des sessions de formation à la sécurité et en vous renseignant sur les tendances, les actualités, les incidents et les bonnes pratiques en matière de cybersécurité. La sophistication et les différents types d'hameçonnage ne cessant de croître et d'évoluer, il est essentiel de rester informé des menaces actuelles.

### 2 - Soyez vigilant et méfiant

Remettez systématiquement en question la légitimité de chaque e-mail, message SMS et appel téléphonique. Si vous recevez un e-mail inattendu d'un collègue, d'un établissement financier, d'une agence gouvernementale ou d'un fournisseur, soyez attentif à ces signes caractéristiques de phishing :

- **Erreurs d'orthographe ou de grammaire :** les fraudeurs incluent intentionnellement des fautes de frappe et de grammaire dans les e-mails de phishing afin de cibler les victimes innocentes et peu méfiantes, tout en éliminant celles qui sont trop intelligentes pour tomber dans le piège. Les fautes de frappe dans les e-mails peuvent contourner les filtres de sécurité ou donner un sentiment d'authenticité au message. En outre, ces erreurs peuvent se produire lorsque l'expéditeur ne maîtrise pas la langue utilisée dans l'e-mail.
- **Demandes urgentes d'informations sensibles :** les e-mails utilisant un langage suscitant un sentiment d'urgence ou de panique visent à inciter les destinataires à agir rapidement sans réfléchir.
- **Liens suspects :** En demandant des informations personnelles ou en téléchargeant des malwares sur votre appareil, les liens de phishing peuvent mener à des sites web suspects.
- **Adresses e-mail usurpées :** bien que les e-mails de phishing semblent provenir d'une source légitime, il est possible de vérifier, en survolant l'adresse e-mail de l'expéditeur, si celle-ci correspond à l'organisation prétendue.
- **Pièces jointes inattendues :** malveillants et nuisant à votre appareil ou volant vos informations, les e-mails de phishing peuvent inclure des pièces jointes inattendues.

### 3 - Utilisez des mots de passe forts et une authentification à deux facteurs

Ajoutez une couche supplémentaire de sécurité à vos comptes en créant des mots de passe uniques et forts et en activant l'authentification à deux facteurs chaque fois que cela est possible. Créez des mots de passe forts en combinant des lettres majuscules et minuscules, des chiffres et des symboles.

Découvrez la solidité de votre mot de passe grâce à l'infographie de Hive System, et utilisez Splashtop Vault pour gérer vos différents identifiants. Vos comptes peuvent être compromis sans que vous le sachiez, il est donc conseillé de changer régulièrement de mot de passe et d'ajouter une deuxième forme d'identification.

### 4 - Maintenez vos logiciels et outils de sécurité à jour

Pour vous protéger contre les menaces les plus récentes, mettez régulièrement à jour les systèmes d'exploitation, les antivirus, les pare-feu et les logiciels anti-malware sur tous vos appareils. Ces mises à jour comprennent des correctifs de sécurité qui corrigent les vulnérabilités connues et vous protègent contre les tentatives de phishing.

### 5 - Ne cliquez jamais sur des liens suspects et ne téléchargez pas les pièces jointes

Avant de cliquer sur des liens ou de télécharger des pièces jointes provenant d'e-mails, de SMS ou autres messages dont l'origine est inconnue, réfléchissez-y à deux fois et survolez le lien à l'aide de votre souris pour vérifier l'URL. Cliquer sur un lien ou une pièce jointe de phishing peut entraîner l'installation d'un logiciel malveillant, un vol de données ou une perte financière.

Si vous recevez un message suspect, vérifiez que l'adresse e-mail ne contient pas de fautes d'orthographe ou un message de salutation générique, et vérifiez la légitimité du contenu auprès de l'expéditeur.

### 6 - Faites attention à vos informations personnelles

Les attaques de phishing vous incitent généralement à fournir des informations personnelles ou financières telles que votre nom d'utilisateur, votre mot de passe ou votre numéro de sécurité sociale. Soyez prudent lorsque vous communiquez des informations en ligne, car les entreprises légitimes ne demandent jamais d'informations par e-mail ou par téléphone.

### 7 - Méfiez-vous de l'usurpation d'identité

Vérifiez si l'adresse e-mail et le nom de l'expéditeur ne sont pas différents. Les signaux d'ingénierie sociale les plus courants sont les suivants :

- Tentatives d'obtention d'informations sensibles
- Demandes de transferts d'argent
- Demandes d'achat inhabituelles ou soudaines
- Changement soudain de dépôt direct

### 8 - Restez prudent sur les réseaux Wi-Fi publics

Évitez d'accéder à des informations sensibles lorsque vous utilisez un réseau Wi-Fi public. Les pirates informatiques peuvent facilement voler des données sur des réseaux non sécurisés.

### 9 - Utilisez des outils de protection contre le phishing

Téléchargez des extensions anti-phishing qui peuvent vous aider à vous protéger contre les attaques d'hameçonnage sur tous vos appareils. Ces outils bloquent l'accès aux sites Web malveillants en analysant les e-mails et les URL à la recherche de formules de phishing connues. Voici quelques outils anti-phishing populaires que vous pouvez utiliser :

- Extension Netcraft : en surveillant les sites Web et en alertant les utilisateurs par un message d'avertissement lorsque des sites suspects sont détectés, cette extension anti-phishing les compare à des bases de données de sites d'hameçonnage.
- Avira Browser Safety : bloquant les sites Web malveillants tels que les sites de phishing, cette extension analyse les téléchargements à la recherche de logiciels malveillants.

- Web of Trust (WOT) : basé sur la fiabilité et la réputation, cette extension avertit les utilisateurs de la mauvaise notoriété d'un site Web.

### 10 - Signalez systématiquement toute activité suspecte

Signalez immédiatement toute tentative de phishing aux autorités compétentes, telles que votre service informatique ou la Fédéral Trade Commission. En signalant ces cas, vous aidez votre service informatique à identifier les menaces potentielles d'hameçonnage afin qu'il puisse prévenir d'autres attaques à l'avenir.

### Pourquoi les employés travaillant à distance sont-ils plus vulnérables aux attaques de phishing ?

Les employés en télétravail sont particulièrement vulnérables aux attaques de phishing pour plusieurs raisons clés :

- Surveillance limitée : les télétravailleurs ne bénéficient souvent pas de la supervision directe de leurs collègues et d'équipes informatiques sur place, ce qui rend plus difficile la détection et le signalement rapide d'activités suspectes.
- Utilisation d'appareils personnels : les appareils personnels et les réseaux domestiques sont généralement moins sécurisés que ceux des systèmes d'entreprise, ce qui augmente le risque de phishing.
- Forte dépendance à l'égard de la communication numérique : le télétravail dépend du courrier électronique, des applications de messagerie et des appels vidéo, qui sont des canaux courants pour les tentatives de phishing. Le volume élevé de communications numériques peut rendre difficile l'identification des messages malveillants.
- Formation à la sécurité réduite : les employés travaillant à distance ont peut-être moins accès à des formations régulières en matière de cybersécurité, ce qui les rend moins bien préparés à reconnaître et à gérer les menaces de phishing.
- Risques accrus liés à l'ingénierie sociale : les interactions fréquentes avec des partenaires et des clients externes offrent de nouvelles opportunités d'attaques d'ingénierie sociale, dans le cadre desquelles les fraudeurs se font passer pour des contacts de confiance.

Il est essentiel de remédier à ces vulnérabilités par le biais de formations ciblées et de mesures de sécurité robustes pour protéger les employés distants contre les attaques de phishing.

### La prévention des attaques de phishing commence par vous

Les attaques de phishing constituent une menace importante pour les particuliers et les organisations. Elles peuvent entraîner des pertes financières, nuire à la réputation et permettre l'accès non autorisé à des informations confidentielles.

Cependant, les employés peuvent atténuer efficacement ces attaques en restant informés, en étant vigilants et en suivant ces conseils et bonnes pratiques. En nous informant et en informant les autres, en restant prudents et en signalant toute activité suspecte, nous pouvons contribuer à prévenir de nouvelles attaques de phishing et à nous protéger, ainsi que nos organisations.