



## Signaler les attaques de phishing aux autorités

Signaler les attaques de phishing aux autorités est une étape cruciale dans la lutte contre la cybercriminalité. Dans cet article, nous verrons pourquoi il est essentiel de signaler les attaques de phishing et nous donnerons un aperçu des défis auxquels les autorités sont confrontées pour attraper les pirates informatiques.

### Pourquoi signaler les attaques de phishing aux autorités ?

- Vous protéger et protéger les autres  
La principale raison de signaler les attaques de phishing est de vous protéger et de protéger les autres contre le même stratagème. Les attaques de phishing peuvent entraîner des pertes financières pour les victimes. Lorsque vous signalez une tentative de phishing, cela permet aux experts en cybersécurité d'analyser l'attaque, d'identifier ses caractéristiques, de créer des contre-mesures, de sensibiliser le public pour empêcher d'autres personnes de se faire avoir par des tactiques similaires, et parfois de saisir des gains illégaux, contribuant ainsi à la récupération des actifs volés.
- Aider à l'action en justice.  
Signaler les attaques de phishing aide la justice à rassembler des preuves et à constituer un dossier contre les cybercriminels. Cela peut conduire à des accusations criminelles, des arrestations et des condamnations, tenant les auteurs responsables de leurs actes. De telles conséquences juridiques ont un effet dissuasif sur les cybercriminels potentiels.

Attention : ne surestimez pas l'action des autorités face au phishing. À moins que vous n'ayez subi une perte financière substantielle, leur action est plutôt limitée. Bien que le

signalement des attaques de phishing soit essentiel, il est important de reconnaître qu'il peut être difficile d'attraper les auteurs pour plusieurs raisons :

- Anonymat : les auteurs de phishing se cachent souvent derrière des couches d'anonymat, ce qui rend difficile la traçabilité de leur véritable identité.
- Problèmes de juridiction : les attaques de phishing peuvent provenir de différents pays, ce qui crée des problèmes de juridiction pour la police et la justice. La coopération internationale implique toujours une tonne de paperasse alors que l'envoi d'un email à travers le monde ne prend que quelques millisecondes.
- Évolution des tactiques : les auteurs de phishing font évoluer constamment leurs tactiques pour garder une longueur d'avance sur les autorités, ce qui en fait un jeu constant du chat et de la souris.
- Ressources limitées : les forces de l'ordre et les organismes judiciaires disposent de ressources limitées pour enquêter sur chaque incident de phishing signalé, en donnant la priorité aux cas les plus importants.

## Comment signaler les attaques de phishing aux autorités ?

- Signalez-les aux agences de cybersécurité.  
De nombreux pays disposent d'agences ou d'unités dédiées chargées de gérer la cybercriminalité. Le tableau suivant en répertorie quelques-unes. Si vous ne trouvez pas d'informations pertinentes pour vous, veuillez rechercher les agences compétentes dans votre pays et suivre leurs procédures de signalement.

Pays	Information	Procédure
Belgique	<a href="https://www.safeonweb.be/fr/liens">https://www.safeonweb.be/fr/liens</a>	Transférez ou envoyez en pièce jointe l'email de phishing à <a href="mailto:suspect@safeonweb.be">suspect@safeonweb.be</a>  Pour le phishing par SMS (smishing), faites une capture d'écran et envoyez-la à <a href="mailto:suspect@safeonweb.be">suspect@safeonweb.be</a>
France	<a href="https://www.signal-spam.fr">https://www.signal-spam.fr</a>	Rendez-vous sur <a href="https://signalants.signal-spam.fr/login">https://signalants.signal-spam.fr/login</a> , créez un compte et suivez la procédure
Allemagne	<a href="https://www.internet-beschwerdestelle.de/en/complaint/submit/e-mail-and-spam.html">https://www.internet-beschwerdestelle.de/en/complaint/submit/e-mail-and-spam.html</a>	Transférez l'email à <a href="mailto:besonderer-spam@internet-beschwerdestelle.de">besonderer-spam@internet-beschwerdestelle.de</a>
UE	<a href="https://www.europol.europa.eu/report-a-crime/report-cybercrime-online">https://www.europol.europa.eu/report-a-crime/report-cybercrime-online</a>	Saisissez le lien du site Web frauduleux sur <a href="https://phishing-initiative.eu/contrib/?lang=fr">https://phishing-initiative.eu/contrib/?lang=fr</a>

Pays	Information	Procédure
Royaume-Uni	<a href="https://www.gov.uk/report-suspicious-emails-websites-phishing">https://www.gov.uk/report-suspicious-emails-websites-phishing</a>	Transférez l'email à <a href="mailto:report@phishing.gov.uk">report@phishing.gov.uk</a> Transférez les SMS au 7726
Suisse	<a href="https://www.post.ch/fr/notre-profil/responsabilite/la-securite-de-l-information-au-sein-de-la-poste/hameconnage-et-autres-tentatives-d-escroquerie">https://www.post.ch/fr/notre-profil/responsabilite/la-securite-de-l-information-au-sein-de-la-poste/hameconnage-et-autres-tentatives-d-escroquerie</a>	Transférez l'email à <a href="mailto:reports@antiphishing.ch">reports@antiphishing.ch</a>
USA	<a href="https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing">https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing</a>	Transférez l'email à <a href="mailto:reportphishing@apwg.org">reportphishing@apwg.org</a> Signalez une tentative de fraude sur <a href="https://reportfraud.ftc.gov/#/assistant">https://reportfraud.ftc.gov/#/assistant</a>

- Signalez-le à la police (ou à un organisme équivalent chargé de l'application de la loi).  
Si vous avez été victime d'hameçonnage et que vous avez subi une perte d'argent ou d'identité, déposez une plainte auprès de la police ou d'un organisme équivalent chargé de l'application de la loi.
- Informez votre banque et vos sociétés de cartes de crédit.  
Si l'attaque de phishing impliquait une fraude financière, contactez immédiatement votre banque et vos sociétés de cartes de crédit. Elles peuvent geler vos comptes et lancer leurs propres enquêtes, ce qui peut compléter les efforts des forces de l'ordre.

## Conclusion

Signaler les attaques de phishing aux autorités est une étape cruciale dans la lutte contre la cybercriminalité. Bien qu'il puisse être difficile d'attraper les pirates de phishing en raison des complexités impliquées, votre signalement peut contribuer à l'effort global de renforcement de la cybersécurité et de protection des individus et des organisations contre ces stratagèmes malveillants. En travaillant ensemble et en signalant rapidement les incidents, nous pouvons contribuer à faire d'Internet un endroit plus sûr pour tous.