



Veille Technologique: LE PHISHING

QU'EST CE QUE LA VEILLE TECHNOLOGIQUE ?

La veille technologique constituée par l'ensemble des techniques visant à organiser de façon systématique la collecte, l'analyse, la diffusion de l'exploitation des informations techniques utiles à la sauvegarde et à la croissance des entreprises. « La veille technologique se doit de prévenir et alerter tout responsable d'un changement, d'une nouveauté ou d'une innovation qu'elle soit technique ou scientifique. Dès lors qu'elle peut modifier le paysage ou faire perdre / gagner un avantage économique, la veille devient critique et doit intervenir le plus tôt possible ».

Pour ma veille technologique j'ai choisi de vous parler du Phishing.

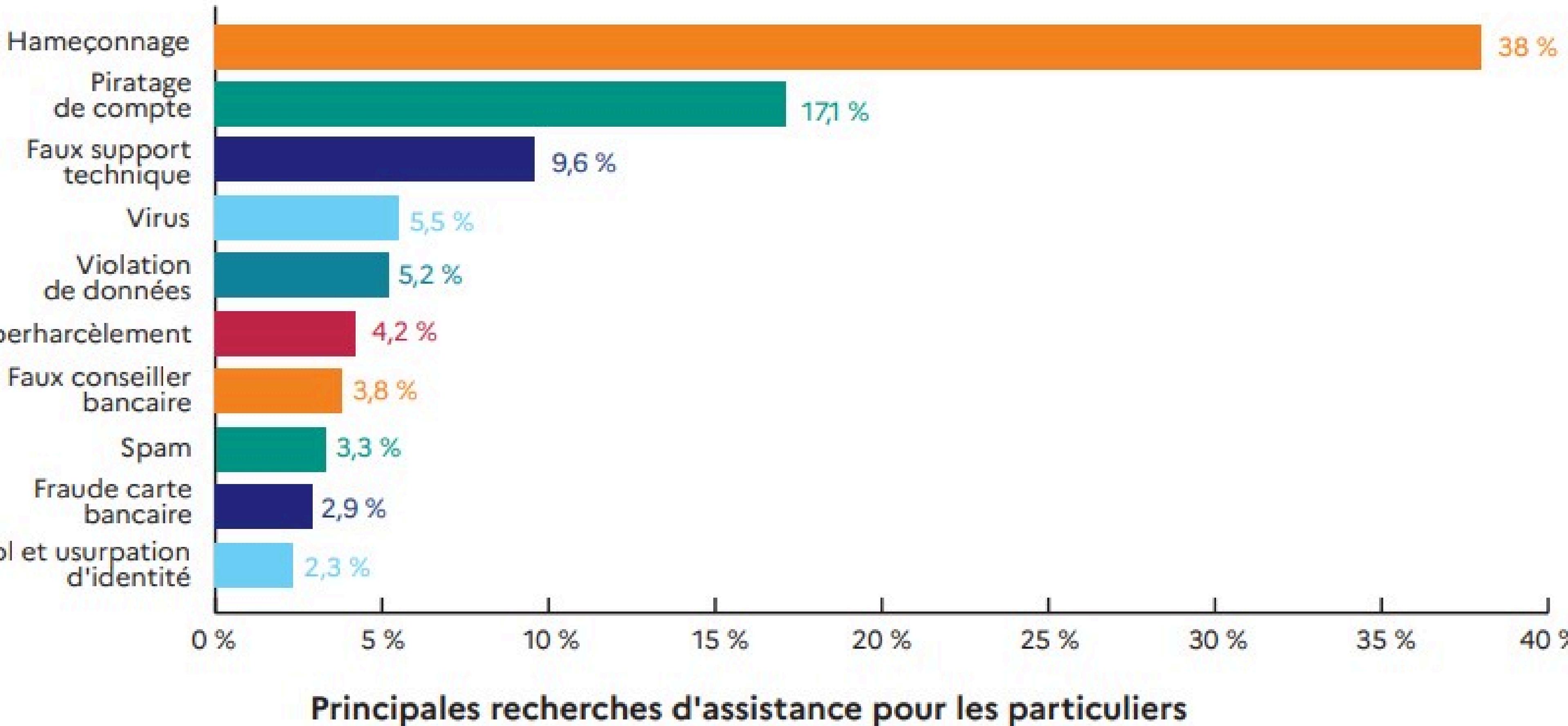


LA CYBERATTAQUE

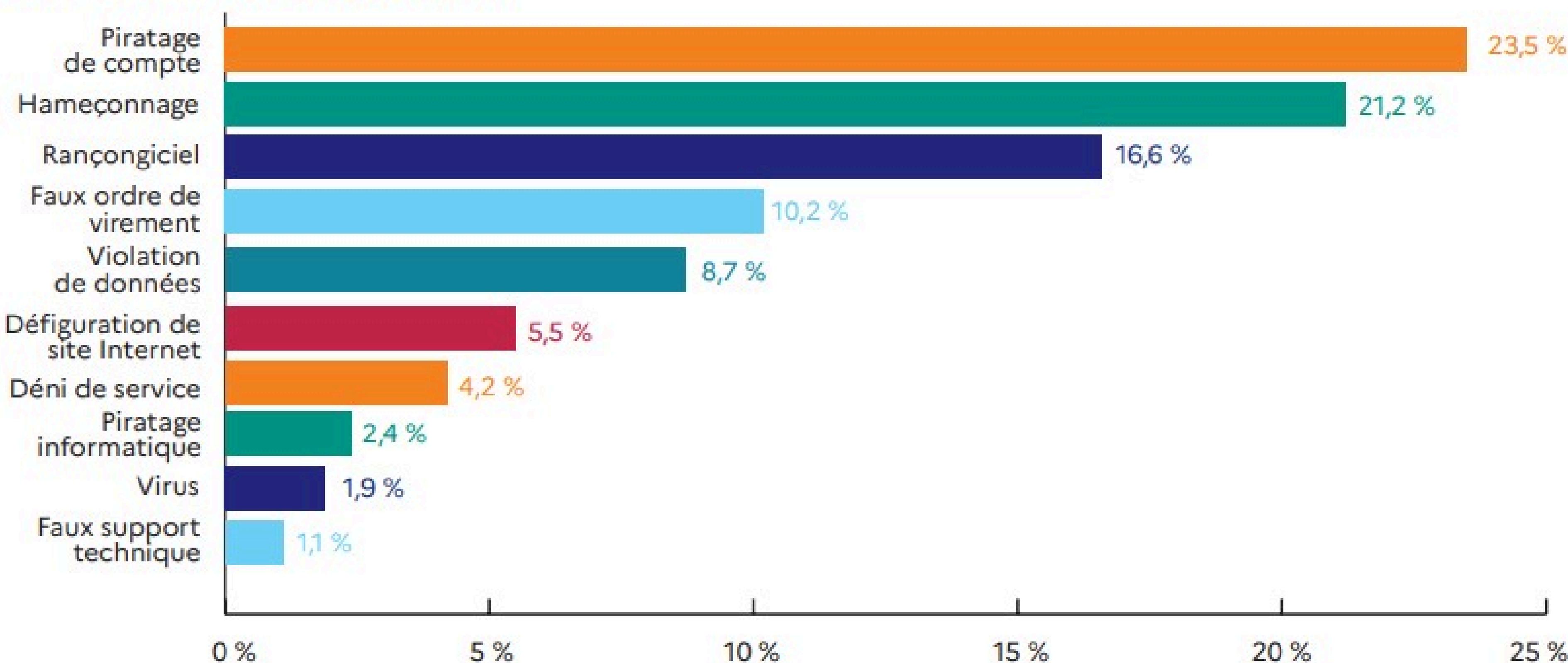
Une cyberattaque est une action malveillante perpétrée à l'aide de technologies informatiques contre des systèmes informatiques, des réseaux, des dispositifs électroniques ou des données numériques. Elle revêt plusieurs formes **en plus du phishing ou hameçonnage qui représente le risque le plus important.**

Les cybercriminels lancent des cyberattaques pour toutes sortes de raisons. Ils utilisent une variété de tactiques, comme les attaques via logiciels malveillants, les arnaques par ingénierie sociale et le vol de mots de passe, pour obtenir un accès non autorisé aux systèmes cibles..

Particuliers



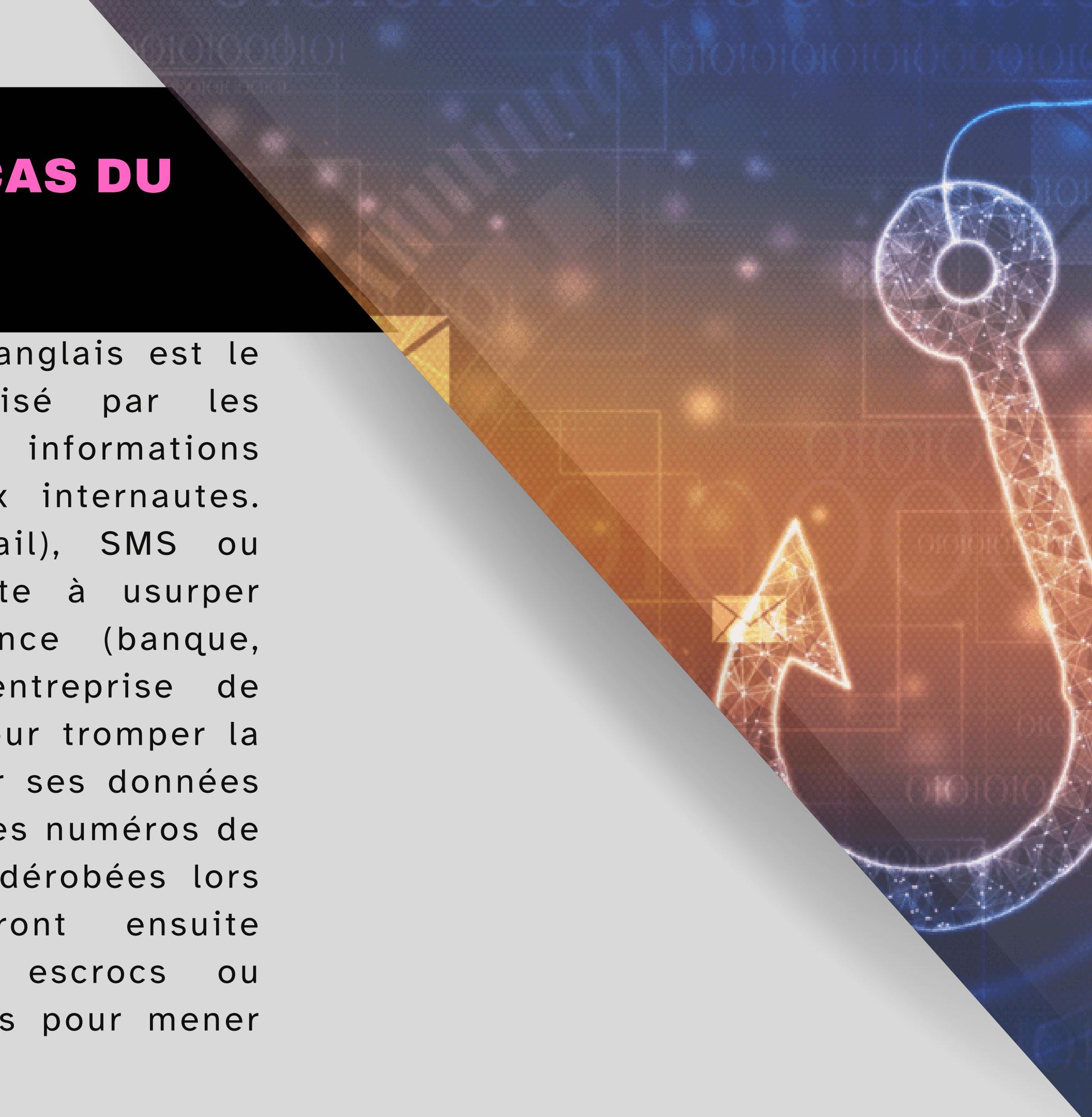
• Entreprises et associations



Principales recherches d'assistance pour les entreprises et les associations

ICI, NOUS ETUDIERONS LE CAS DU PHISHING

L'hameçonnage ou phishing en anglais est le principal mode opératoire utilisé par les cybercriminels pour dérober des informations personnelles et/ou bancaires aux internautes. Par message électronique (e-mail), SMS ou encore par téléphone, il consiste à usurper l'identité d'un tiers de confiance (banque, administration, réseau social, entreprise de livraison, commerce en ligne...) pour tromper la victime et l'inciter à communiquer ses données d'identité, ses mots de passe ou ses numéros de carte bancaire. Les informations dérobées lors de l'hameçonnage/phishing seront ensuite directement utilisées par les escrocs ou revendus à d'autres cybercriminels pour mener diverses actions frauduleuses.



CONTEXTE HISTORIQUE

Le terme "phishing" vient du mot "fishing" (pêche en anglais), car les cybercriminels "attrapent" des informations sensibles en envoyant de faux messages ou en créant des sites Web frauduleux. L'orthographe "ph" remplace le "f" pour imiter les termes techniques de l'informatique (comme "phreaking", qui désignait l'art de pirater les lignes téléphoniques).

Les premières attaques de phishing ont eu lieu dans les années 1996 à 1998. À cette époque, les pirates informatiques ciblaient principalement les utilisateurs d'AOL (America Online), un fournisseur d'accès à Internet populaire aux États-Unis. Ils envoyoyaient de faux e-mails prétendant provenir d'AOL, demandant aux utilisateurs de fournir leurs identifiants de connexion sous prétexte de vérifier leur compte ou de résoudre un problème technique.

Le phishing repose sur des techniques d'ingénierie sociale, où **les cybercriminels manipulent les utilisateurs en jouant sur leurs émotions, leur confiance ou leur peur**. Les messages sont souvent conçus pour provoquer une réaction rapide, comme la peur d'une suspension de compte ou d'une offre spéciale trop alléchante pour être ignorée.

Avec l'avènement des réseaux sociaux, du commerce en ligne et de services numériques divers, le phishing s'est adapté. **Il peut désormais prendre la forme de messages sur les réseaux sociaux, de SMS (smishing), ou de messages vocaux (vishing), en plus des e-mails traditionnels.**

Selon le rapport annuel de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), le nombre d'attaques signalées a augmenté de 15 % par rapport à 2023, avec une hausse particulière des attaques par phishing et ransomware.

QUELS SONT LES PRINCIPAUX ACTEURS DU PHISHING ?

- 01 Cybercriminels individuels**
- 02 Groupes de hackers organisés**
- 03 États et acteurs sponsorisés par des gouvernements**



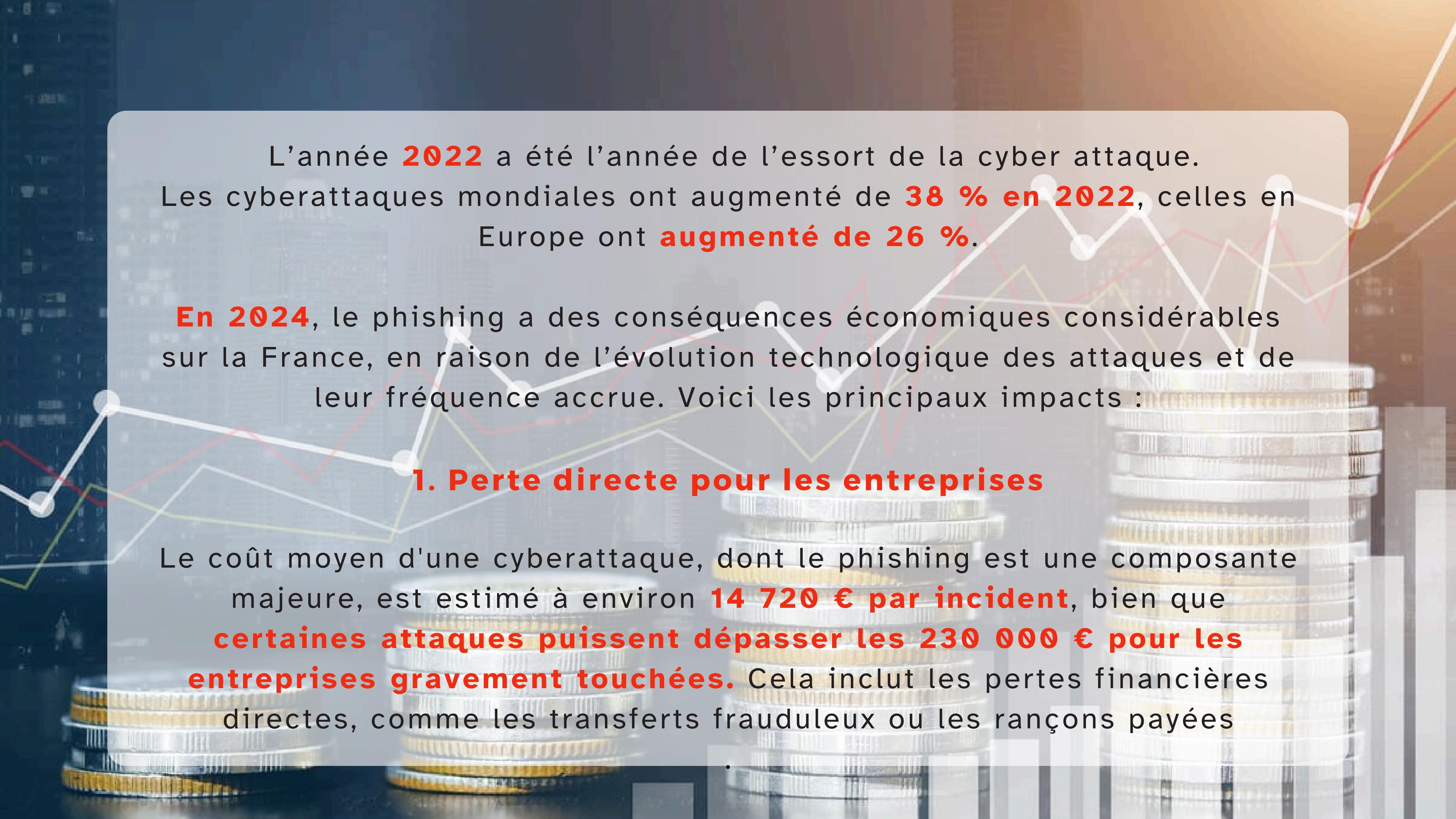
Cependant, qu'ils agissent de l'un ou de l'autre, n'importe qui peut lancer des cyberattaques. C'est pourquoi on classe plutôt les cybercriminels en menaces externes ou internes.

Les menaces extérieures ne sont pas autorisées à utiliser un réseau ou un appareil, mais s'y introduisent quand même. Parmi ces menaces, on compte les groupes criminels organisés, les pirates informatiques professionnels, les acteurs sponsorisés par les États, les pirates amateurs et les hacktivistes.

Les menaces internes correspondent aux utilisateurs qui ont un accès autorisé et légitime aux actifs d'une entreprise et abusent de leurs priviléges délibérément ou accidentellement. Cette catégorie comprend le personnel, les partenaires commerciaux, les clients, les prestataires et les fournisseurs ayant accès au système.

CONSEQUENCES ECONOMIQUES DU PHISHING SUR LA FRANCE





L'année **2022** a été l'année de l'essor de la cyber attaque. Les cyberattaques mondiales ont augmenté de **38 % en 2022**, celles en Europe ont **augmenté de 26 %**.

En 2024, le phishing a des conséquences économiques considérables sur la France, en raison de l'évolution technologique des attaques et de leur fréquence accrue. Voici les principaux impacts :

1. Perte directe pour les entreprises

Le coût moyen d'une cyberattaque, dont le phishing est une composante majeure, est estimé à environ **14 720 € par incident**, bien que **certaines attaques puissent dépasser les 230 000 € pour les entreprises gravement touchées**. Cela inclut les pertes financières directes, comme les transferts frauduleux ou les rançons payées

2. Perturbation des activités

- Les attaques de phishing entraînent des interruptions opérationnelles significatives, telles que des systèmes informatiques inaccessibles, la perte de données ou des retards dans les opérations commerciales. Ces interruptions affectent les revenus des entreprises, en particulier les PME, souvent moins équipées pour gérer de telles crises.

3. Amendes réglementaires et atteinte à la réputation

- Les violations de données issues de campagnes de phishing exposent les entreprises à des sanctions prévues par le RGPD, en plus de nuire à leur image de marque. Les clients et partenaires peuvent perdre confiance, ce qui complique l'acquisition de nouveaux contrats et la fidélisation de la clientèle.

Phishing Attacks by Industry Vertical

Technology

4.1%

Services

5.7%

Retail Wholesale

6.4%

Manufacturing

8.8%

Health Care

8.9%

Other

10.5%

Education

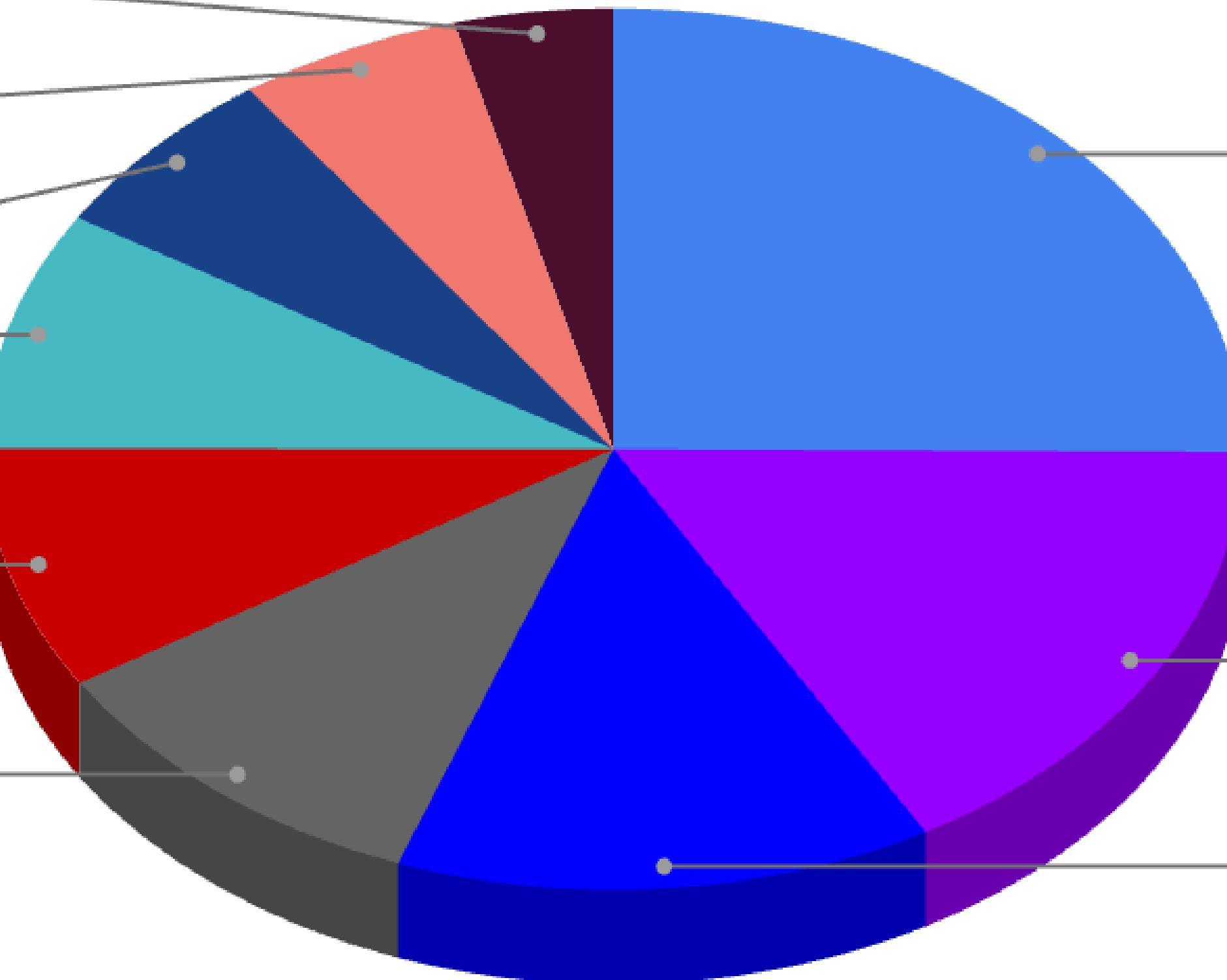
25.1%

Finance Insurance

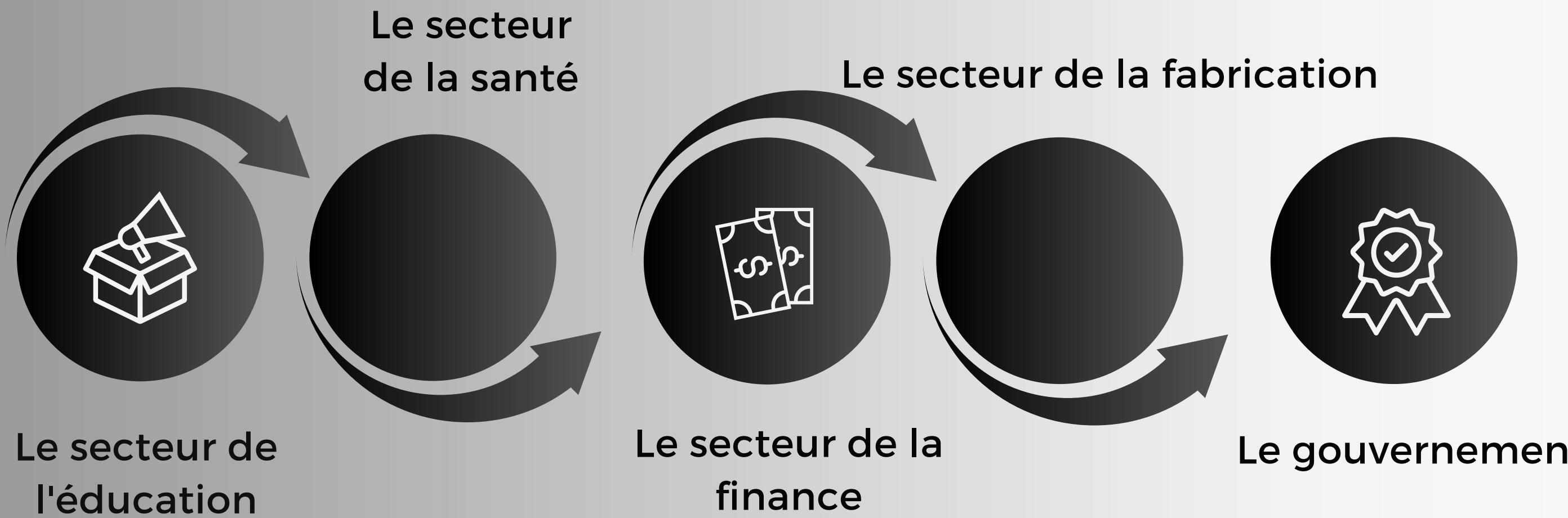
16.6%

Government

13.8%



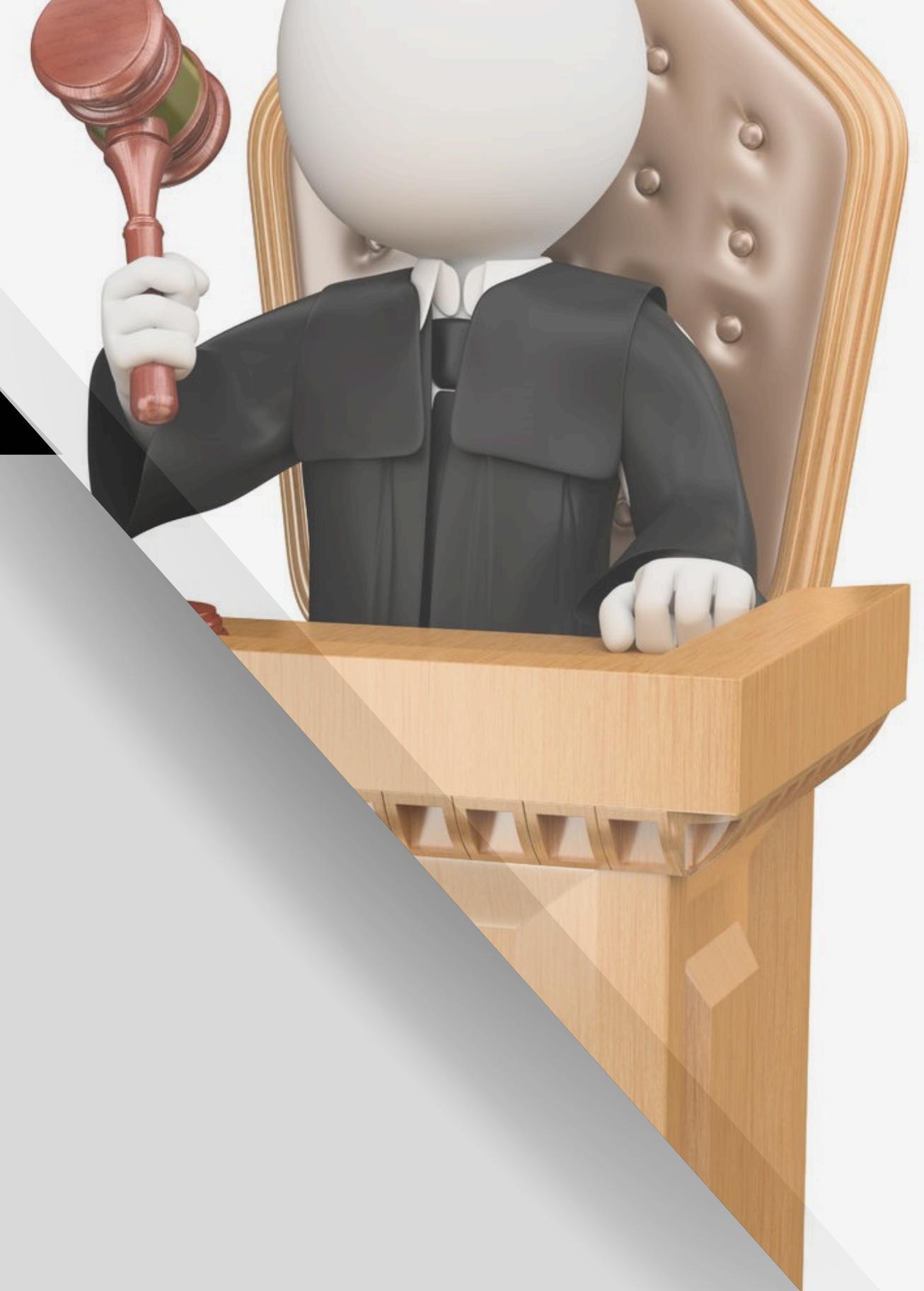
Les secteurs les plus ciblés

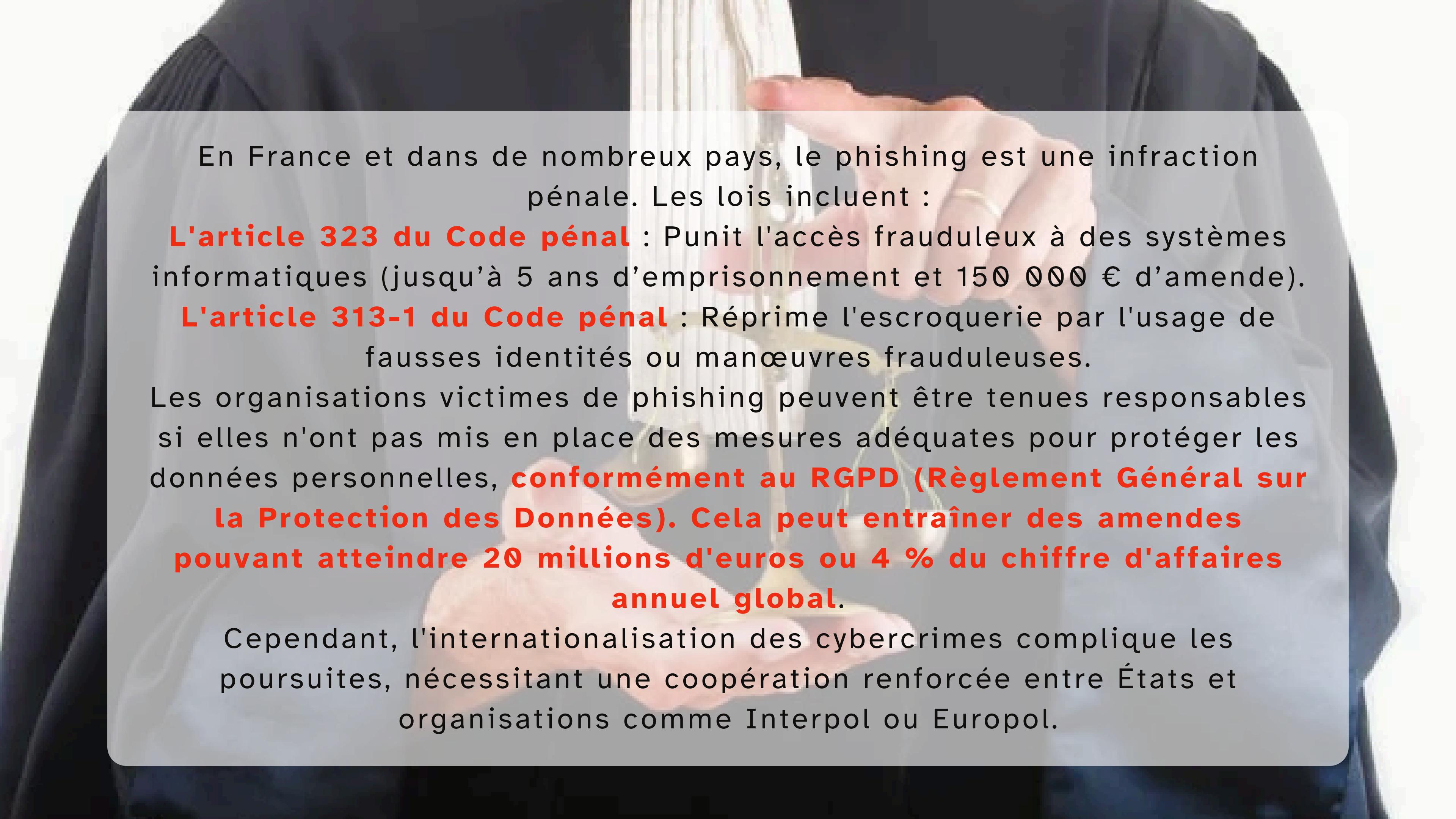


PORTEE ETHIQUE ET JURIDIQUE DU PHISHING

Le phishing repose sur la tromperie pour exploiter la confiance des individus ou des organisations. Cela constitue **une violation flagrante des principes d'intégrité et d'honnêteté**, essentiels dans les relations humaines et professionnelles.

Les cybercriminels ciblent souvent des groupes vulnérables, comme les personnes âgées ou les non-experts en technologie, ce qui pose des questions éthiques sur **l'abus des désavantages sociaux ou cognitifs**. De plus, il contribue à une érosion de la confiance dans les interactions numériques, freinant l'adoption de nouvelles technologies et amplifiant **la méfiance envers les institutions légitimes, comme les banques ou les gouvernements**.





En France et dans de nombreux pays, le phishing est une infraction pénale. Les lois incluent :

L'article 323 du Code pénal : Punit l'accès frauduleux à des systèmes informatiques (jusqu'à 5 ans d'emprisonnement et 150 000 € d'amende).

L'article 313-1 du Code pénal : Réprime l'escroquerie par l'usage de fausses identités ou manœuvres frauduleuses.

Les organisations victimes de phishing peuvent être tenues responsables si elles n'ont pas mis en place des mesures adéquates pour protéger les données personnelles, **conformément au RGPD (Règlement Général sur la Protection des Données). Cela peut entraîner des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel global.**

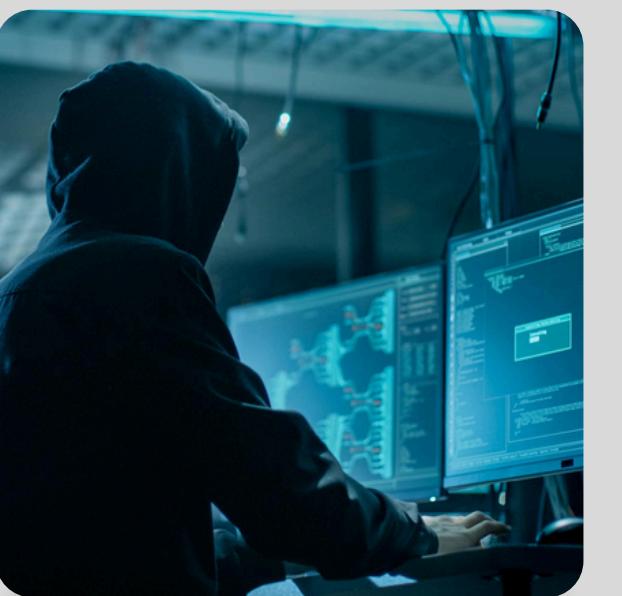
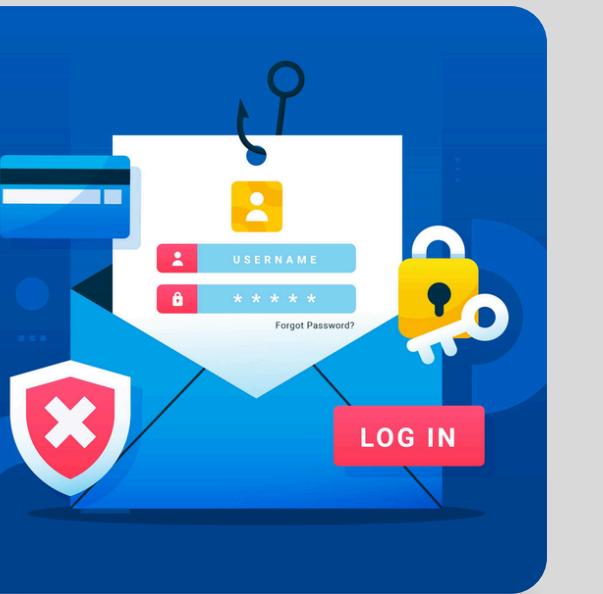
Cependant, l'internationalisation des cybercrimes complique les poursuites, nécessitant une coopération renforcée entre États et organisations comme Interpol ou Europol.

CONCLUSION

Pour conclure, nous dirons que le phishing contribue à un climat d'insécurité numérique, ralentissant la transition numérique des entreprises et pesant sur leur compétitivité. On estime que **la fréquence des attaques a augmenté de 58 % entre 2023 et 2024**, ce qui intensifie les pertes globales pour l'économie française.

Pour réduire ces impacts, il est crucial que les entreprises adoptent des solutions de cybersécurité robustes, renforcent la formation de leurs employés sur les pratiques numériques sécurisées, et mettent en place des plans de réponse aux incidents. Cela nécessite une collaboration entre le secteur privé, les gouvernements, et les experts en cybersécurité.





SOURCES

- Forbes France
- GOOGLE alert
- L'ANSSI
- Data.gouv.fr
- Intelekto