ANTI-PHISHING

Comment naviguer en eaux sûres ?

Le courrier électronique fait partie du quotidien des collaborateurs en entreprise. A ce titre, il constitue un vecteur particulièrement choyé par les cyber-attaquants, à travers la méthode de phishing BEC (Business email compromission). Malgré les actions et les outils de défense déployés au sein des organisations et des entreprises, le phishing ne faiblit pas, en France comme dans le reste du monde. Pour quelles raisons ? Selon quelle intensité et quelles modalités ? Quels types de solutions les entreprises et organisations ont-elles mis ou devraient-elles mettre en place pour contrer ces menaces et se protéger ? Quel est le degré de maturité des entreprises à l'égard du phishing ?

Cloudflare a recueilli l'opinion de 100 décideurs et responsables IT d'entreprises de plus de 500 salariés, tout secteur, en juin et juillet 2023, dans le cadre de la 1re édition du baromètre Phishing de Cloudflare en France.

SOMMAIRE :

Introduction

RAPPEL

Le phishing, également connu sous le nom d'hameçonnage, est une technique d'escroquerie en ligne utilisée par des individus malveillants pour tromper les personnes et accéder ainsi à des informations personnelles, telles que des identifiants de connexion, des informations financières, des numéros de carte de crédit, ou d'autres données sensibles. Les attaquants se font passer pour des entités de confiance, telles que des institutions financières, des entreprises légitimes, des gouvernements, ou même des individus, dans le but de convaincre leurs cibles de partager ces informations.

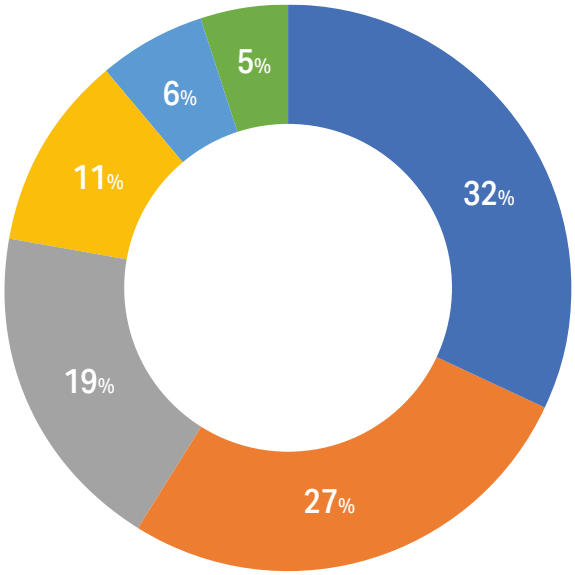
Le phishing peut se produire via divers canaux, notamment par e-mail, messagerie instantanée, messages texte, réseaux sociaux, sites web frauduleux, ou même par téléphone. Les messages de phishing sont conçus pour ressembler à des communications légitimes, avec des logos, des noms d'entreprise et des informations qui semblent authentiques, afin de leurrer les victimes.

OBJECTIF DES CYBER-ATTAQUANTS

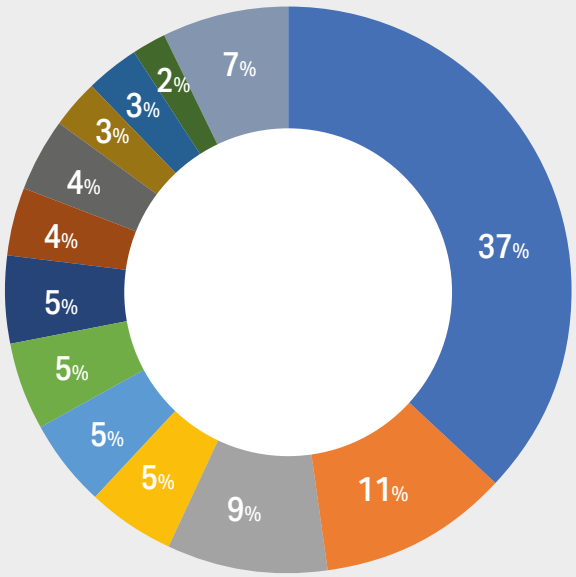
Utiliser ces informations à des fins frauduleuses, telles que le vol d'argent, l'usurpation d'identité, ou d'autres activités illicites.

Point graphique sur le profil des répondants

Plus d'un tiers des répondants (37 %) est issu du secteur de l'industrie et un cinquième (20 %) du secteur des services (banques, assurances, services aux entreprises). Cette forte représentation de secteurs extrêmement vulnérables et sensibles au phishing traduit leur intérêt à l'égard de ces enjeux.



- DSI
- Informatique
- Sécurité
- Infrastructure
- Système et réseau
- Autre : Opération, parc, Production, Support



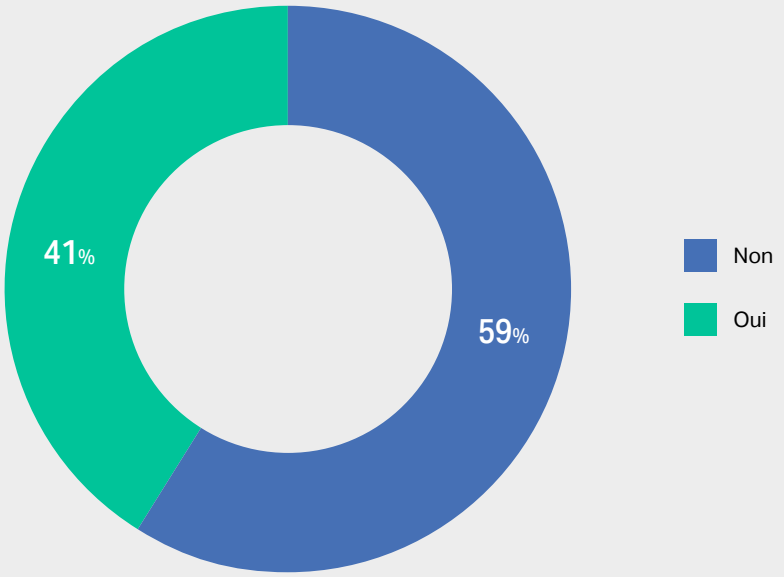
SECTEURS

- Industrie
- Service aux entreprises
- Banque/Assurance
- Agroalimentaire
- Immobilier
- Technologies et services de l'information
- Transport
- Commerce

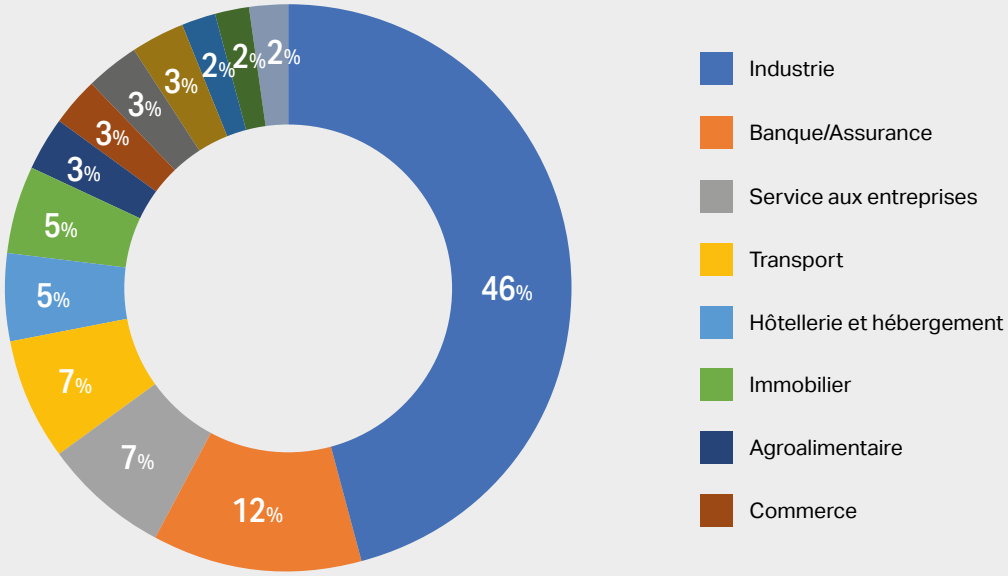
1 Principales tendances

- Seulement **41 %** des répondants déclarent avoir été l'objet d'attaques avancées de phishing, type BEC, alors que **71 %** des entreprises ont été l'objet de ce type d'attaques en 2023.
- Principal risque encouru : les pertes financières (**32 %**), devant la fuite des données (**27 %**) et le ralentissement de l'activité (**27 %**).
- **94 %** des répondants déclarent que leur organisation est équipée d'une solution anti-phishing.
- Les solutions natives de Google et Microsoft plus souvent citées que tout autre solution.
- **72 %** des DSI plébiscitent les programmes de formation mixant sensibilisation et outils dédiés .

2 Phishing : rien à déclarer ?



SECTEURS AYANT RÉPONDU OUI



Plus de la moitié des répondants (**59 %**) déclare ne pas avoir été l'objet d'attaques avancées de phishing, type BEC (Business email compromise, ou compromission du courrier électronique professionnel), contre **41 %**. Une part étonnamment importante dans la mesure où dans une autre étude réalisée en 2023, **71 %** des entreprises déclaraient avoir été l'objet d'une attaque, type BEC, contre **29 %**. Un différentiel important qui peut s'expliquer par le profil des répondants : les DSI, fortement représentés dans notre échantillon de répondants, n'ont peut-être pas encore acquis une culture de transparence à l'égard des attaques dont leur organisation a été l'objet.

Inversement, sans surprise, les secteurs se montrant les plus transparents quant au fait d'avoir déjà été victimes d'une attaque sont les plus vulnérables et les plus exposés, donc les plus sensibilisés aux démarches de phishing – c'est-à-dire ceux dont on peut penser qu'ils sont les plus enclins à déclarer ouvertement avoir été victimes d'un phishing. C'est pourquoi on trouve loin devant le secteur de l'industrie (**46 %**), ceux de la banque-assurance (**12 %**), des services aux entreprises (**7 %**) et des transports (**7 %**).

En termes de fréquence d'attaques, **19%** des répondants déclarent subir des attaques plus d'une fois par mois – **27 %** dans le secteur de l'industrie, signe supplémentaire d'une plus forte vulnérabilité au sujet de la part de ce secteur.

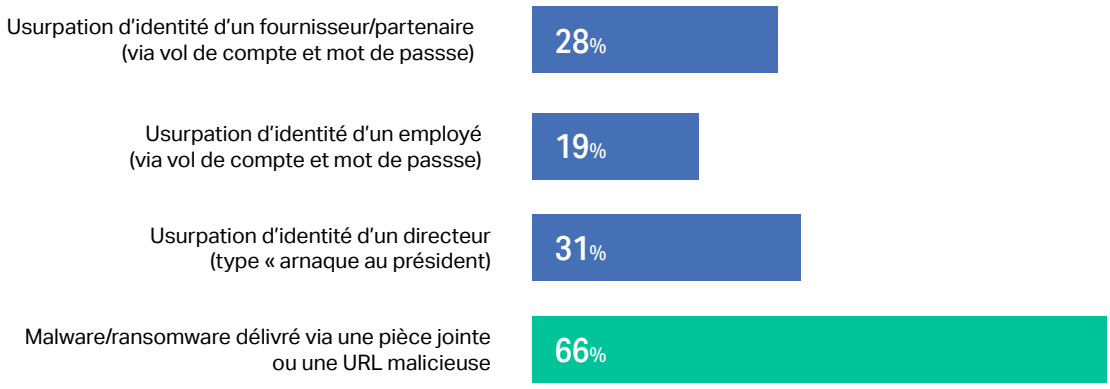
3 Usurpation d'identité & URL malicieuse : procédés perçus comme les plus dangereux par les DSI

Parmi les types d'attaques considérés comme les plus dangereux, deux tiers (**66 %**) des répondants citent le malware/ransomware via une pièce jointe ou une URL malicieuse, loin devant l'usurpation d'identité d'un directeur (**31 %**), ou d'un fournisseur-partenaire (**28 %**) ou celle d'un collaborateur (**19 %**).

Une étude menée par Cloudflare montre que les attaques via pièces jointes sont de moins en moins fréquentes, en raison d'une progressive accoutumance des salariés à s'en méfier. La menace via pièce jointe est désormais très faiblement utilisée par les acteurs malveillants (**1,9 %**), à l'inverse de l'URL malicieuse (**35,6 %**), moins détectable.

Constat partagé par les DSI : à leurs yeux, parmi un certain nombre de menaces, la pièce jointe suspecte constitue l'indicateur de phishing le moins susceptible d'attirer l'attention des collaborateurs (**17 %**), loin derrière des courriels usurpant l'identité d'une entreprise de confiance (**39 %**) ou contenant une URL suspecte (**31 %**).

Si on met de côté l'URL malicieuse, l'usurpation d'identité reste à ce jour, selon notre étude, le type d'attaque le plus redouté par les DSI, que ce soit l'arnaque au président (**31 %**), ou celle au fournisseur/partenaire (**28 %**).

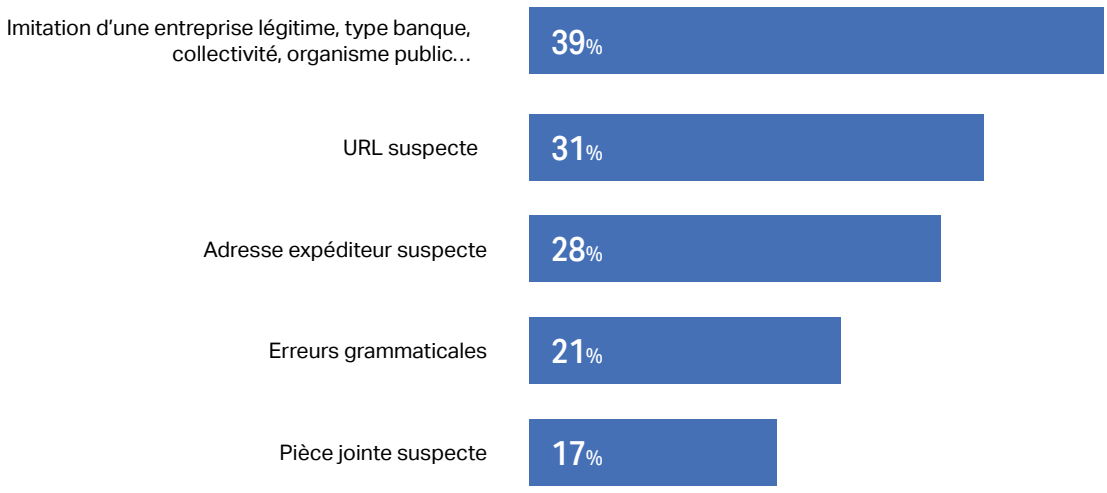


4 Les collaborateurs : quelles failles ?

Aux yeux des DSI, l'indicateur de phishing considéré comme le vecteur d'attaque le plus dangereux est celui de l'usurpation d'identité, qu'elle soit celle d'une entreprise légitime (fournisseur, partenaire), d'une banque ou d'une collectivité (**39 %**). Une donnée confirmée dans le rapport Cloudflare 2023 : elles représentent **14,2 %** des attaques détectées, constituent le 3e type d'attaques le plus couramment usité, et connaissent un bond de plus de **10 %** par rapport à 2022.

Deuxième confirmation : le faible danger représenté par les pièces jointes suspectes (**17 %**), de moins en moins d'attaques n'étant constituées que d'un malware en pièce jointe d'un email, car celles-ci sont désormais de plus en plus facilement détectables.

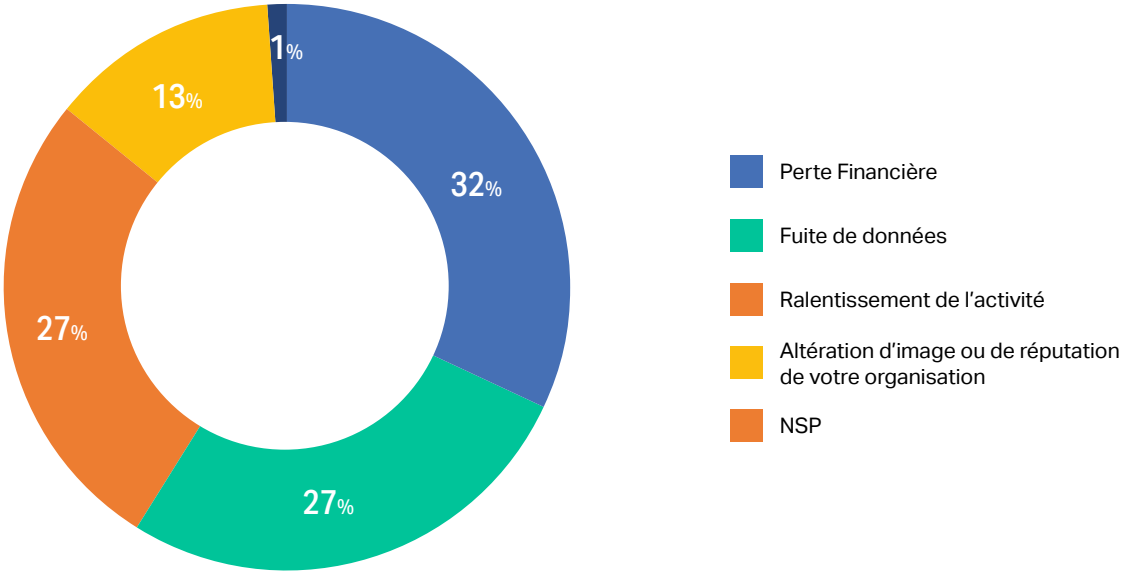
Troisième confirmation : la prise en considération de l'URL malicieuse comme nouvelle menace (**31 %**). En effet, l'un des moyens par lesquels un cyber-attaquant peut imiter l'identité d'une marque consiste à utiliser un domaine récemment enregistré (NRD, Newly registred domain). Or comme le montre le rapport Cloudflare déjà mentionné, les menaces dues à l'âge du domaine représentent désormais la 2e catégorie de menace, détectée dans **30 %** des mails indésirables.



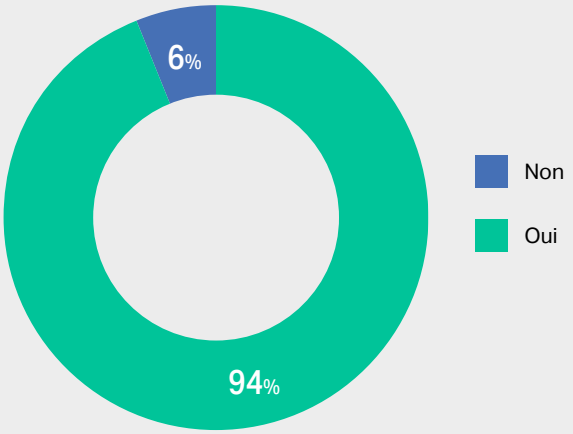
5 Risques redoutés : d'abord l'impact technique et financier, loin devant la réputation

Pertes financières (**32 %**), fuite de données (**27 %**) et ralentissement de l'activité (**27 %**), tels sont les principaux risques encourus par les organisations, selon les répondants. Notons que le risque réputationnel (altération d'image), avec **13 %** de citations, arrive loin derrière, ce qui traduirait soit le signe d'une faible maturité à l'égard de ces enjeux, soit au contraire le fait qu'une sensibilisation sur ce sujet ait déjà été effectuée.

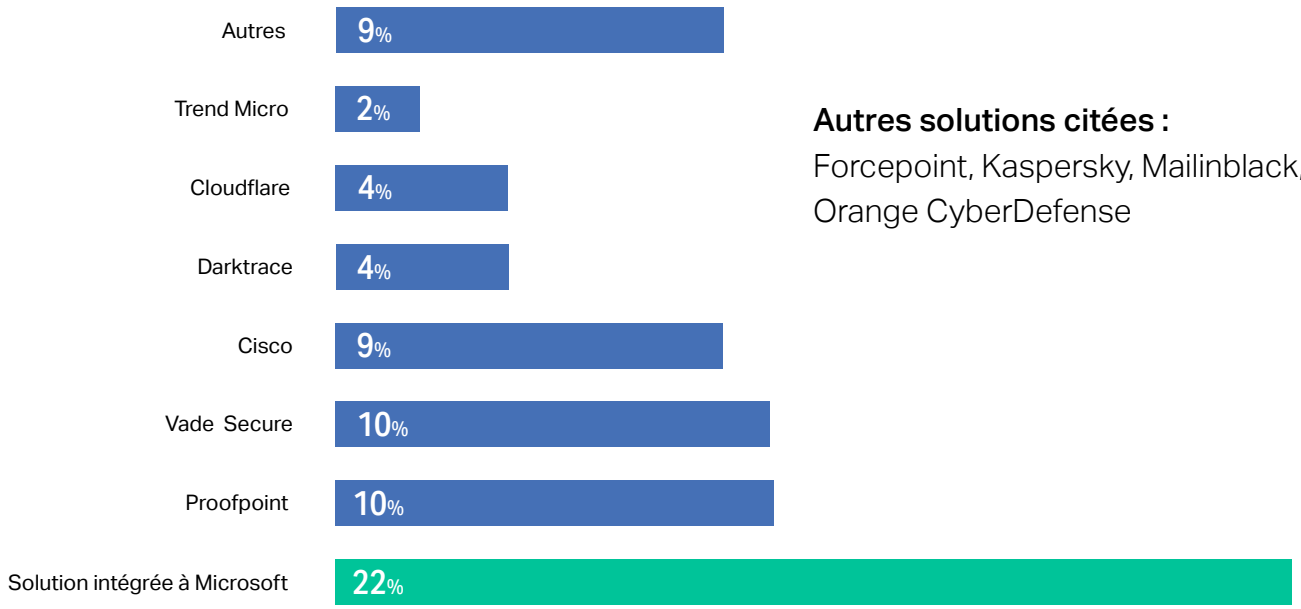
Par type d'activité, les risques encourus ne sont pas de même nature. Dans le secteur industriel, c'est le ralentissement de l'activité qui est d'abord redouté (**41 %**), devant les pertes financières (**35 %**), la fuite des données (**13 %**) et l'altération d'image (**11 %**). Pour les banques, la fuite de données (**56 %**) précède largement des pertes financières (**33 %**) et l'altération d'image (**11 %**).



6 Bien équipé, bien protégé ? Le paradoxe du phishing



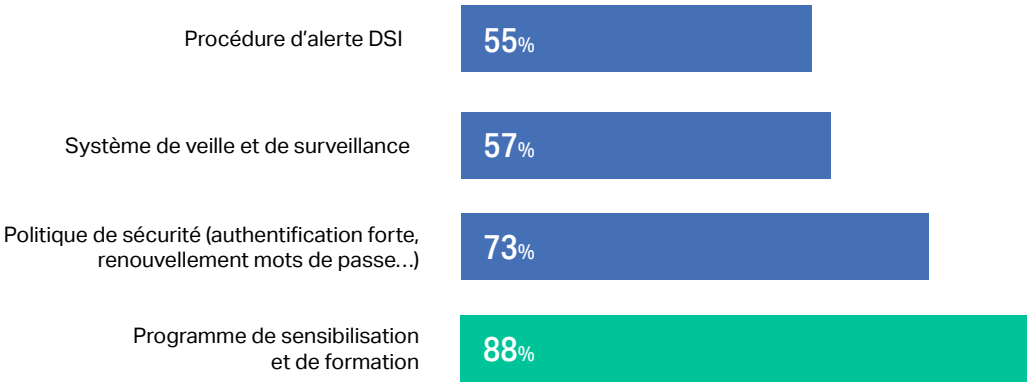
Paradoxalement, malgré ce contexte de craintes, les répondants se disent dans une très large proportion (**94 %**) équipés d'une solution de lutte contre le phishing.



Autres solutions citées :
Forcepoint, Kaspersky, Mailinblack, Orange CyberDefense

Or ce paradoxe n'est qu'apparent. En effet, on peut émettre l'hypothèse que cette très forte proportion provient du fait qu'ils sont équipés d'une solution native à leur navigateur. C'est le type de solution qui est le plus largement cité (**22 %**), devant des solutions externes, type Proofpoint (**10 %**), VadeSecure (**10 %**), Darktrace (**4 %**) et Cloudflare (**4 %**)
Or ces premières lignes de défense Google et Microsoft, obligatoires, ne sont aujourd'hui ni suffisantes ni adaptées pour contrer les cybermenaces de plus en plus sophistiquées.

7 Lutte contre le phishing : priorité au mix sensibilisation-solutions



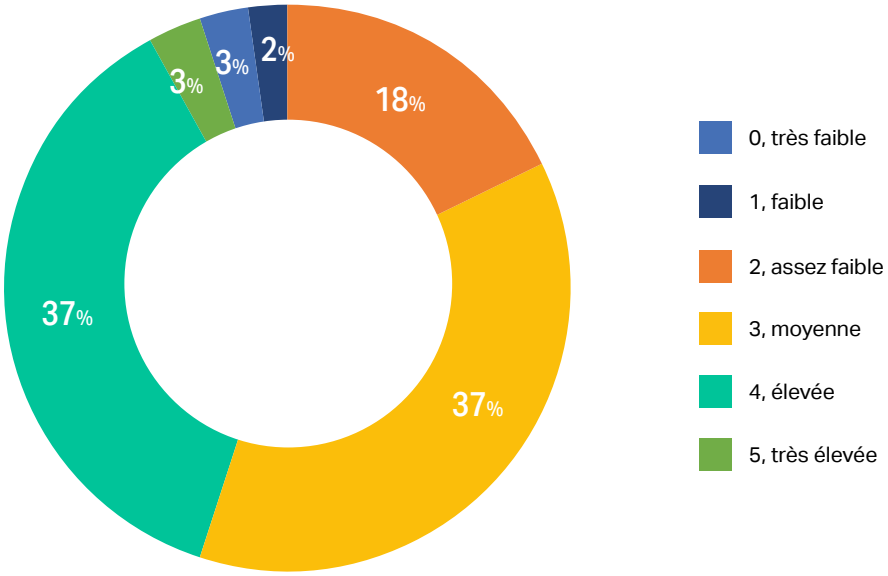
72 % ont répondu une combinaison de plusieurs mesures et **43 %** d'entre eux ont notamment coché toutes les mesures possibles ; **21 %** ont seulement mis en place un programme de formation.

En matière de lutte contre le phishing, il apparaît que les entreprises ont mis en place un mix entre sensibilisation et solutions de protection anti-phishing – les répondants étant amenés à choisir plusieurs réponses : **43 %** d'entre eux ont coché toutes les options proposées, **72 %** une combinaison d'au moins deux options, **21 %** seulement un programme de sensibilisation.

La part prédominante des programmes de sensibilisation et de formation (88 %) peut s'expliquer selon deux facteurs :

- Soit par l'intégration du déploiement de solutions anti-phishing, propres au programme de sensibilisation-formation
- Soit par la dimension incompressible du facteur humain inhérente aux incidents liés aux violations de données. Selon le rapport 2023 Data Breach Investigations de Verizon, le facteur humain joue un rôle dans **74 %** des violations IT. Ce qui nécessite une adaptation constante et continue de ces programmes, en fonction de l'évolution des menaces qui visent les vulnérabilités des entreprises à travers les failles humaines.

8 La maturité phishing : disparate selon les secteurs



Au final, si **23 %** des répondants estiment le degré de maturité des collaborateurs en entreprise faible ou très faible, **40 %** l'estiment élevé ou très élevé.
La sensibilisation aux enjeux de cybersécurité semble donc bien engagée. Mais ce mouvement n'est cependant pas uniforme selon les secteurs les plus vulnérables : dans le secteur bancaire, le degré de maturité est jugé élevé ou très élevé par **56 %** des répondants, là où il ne l'est qu'à hauteur de **35 %** dans le secteur industriel.

9 Conclusion

Notre baromètre révèle que des efforts en matière de lutte contre le phishing ont été accomplis. Ainsi, les menaces liées aux pièces jointes sont désormais considérées comme mineures. Mais la menace persistante du phishing type URL malicieuse exige une vigilance constante.

C'est là le principal enjeu qui se pose aux DSI : alors qu'ils se déclarent protégés et équipés de solutions anti-phishing, ils doivent contrer des menaces en recrudescence, de plus en plus sophistiquées. Et ce, dans un contexte où la sensibilisation à l'égard du phishing progresse, notamment à travers la mise en place de programmes de formation, bien que disparate selon les secteurs d'activité.

Cloudflare offre des solutions adaptées pour renforcer la cybersécurité. Contactez-nous pour naviguer en eaux sûres et renforcer votre arsenal contre le phishing.

Cloudflare offre des solutions adaptées pour renforcer la cybersécurité. Contactez-nous pour naviguer en eaux sûres et renforcer votre arsenal contre le phishing.

10 Contactez-nous

Vous êtes concerné
par le phishing ?

Vos défenses actuelles vous semblent faiblement opérantes ?

Vous souhaitez en savoir plus
sur nos solutions et approches ?

CONTACTEZ-NOUS

Boris Lecoeur, DG France
blecoeur@cloudflare.com

Cloudflare est une plateforme zero trust 100 % cloud qui connecte et protège les collaborateurs, les applications et les données partout dans le monde. Cloudflare protège 20 % des sites web dans le monde contre les attaques cyber grâce à son réseau mondial présent dans 310 villes réparties dans 120 pays. Le réseau s'interconnecte à plus de 13 000 réseaux à travers le monde, notamment ceux des principaux FAI, services cloud et entreprises. La plateforme Cloudflare permet à ses clients de rendre leurs collaborateurs, leurs applications et leurs réseaux plus rapides et plus sûrs, tout en réduisant la complexité et les coûts. La solution Cloudflare de connectivité cloud propose la plateforme unifiée la plus complète en matière de produits et d'outils de développement cloud-native, permettant à toutes les entreprises d'accéder au contrôle dont elles ont besoin pour travailler, développer et accélérer leur activité. Cloudflare bloque chaque jour 170 milliards de menaces par jour.