proofpoint

Europe et Moyen-Orient

RAPPORT

State of the Phish 2024

Actions dangereuses, menaces réelles et résilience des utilisateurs à l'ère de la cybersécurité centrée sur les personnes

proofpoint.com/fr

INTRODUCTION

Bien souvent, les gros titres se concentrent sur les stratégies astucieuses d'ingénierie sociale et les vulnérabilités « zero-day » utilisées par les cybercriminels. Mais ces derniers n'ont pas toujours besoin de déployer tant d'efforts. D'après l'enquête State of the Phish 2024, 71 % des adultes actifs ont admis avoir effectué une action dangereuse, comme réutiliser ou partager un mot de passe, cliquer sur des liens envoyés par des expéditeurs inconnus ou divulguer des identifiants de connexion à une source non fiable. 96 % d'entre eux l'ont fait en sachant qu'ils prenaient un risque. Les personnes sont une composante essentielle de toute stratégie de défense efficace, mais elles peuvent aussi en être le maillon le plus vulnérable. Elles peuvent commettre des erreurs, tomber dans le piège d'escrocs ou simplement ignorer les bonnes pratiques de sécurité.

Le rapport mondial 2024 s'appuie sur une enquête menée auprès de 7 500 utilisateurs et 1 050 professionnels de la sécurité dans 15 pays, dont huit en Europe et au Moyen-Orient. Il inclut également des données Proofpoint issues de nos produits et recherches sur les menaces, ainsi que des conclusions reposant sur 183 millions de messages de simulation d'attaque de phishing envoyés par nos clients sur une période de 12 mois et plus de 24 millions d'emails signalés par les utilisateurs de nos clients sur la même période. Pour la deuxième année consécutive, nous avons compilé trois synthèses régionales mettant en lumière les nuances et variations locales.

La plupart des utilisateurs en Europe et au Moyen-Orient ne savent pas si la sécurité relève de leur responsabilité ou de celle de quelqu'un d'autre. Ce manque de clairvoyance peut avoir des conséquences désastreuses. Nos données montrent des corrélations saisissantes entre les attitudes et les résultats dans l'ensemble de la région.

Chaque jour, les utilisateurs de la région font des choix entre sécurité et commodité. Cette synthèse régionale montre que la plupart du temps, ils privilégient la commodité. Dans les pages suivantes, nous nous intéresserons de plus près aux attitudes des professionnels de la sécurité et des utilisateurs, ainsi qu'à certaines tendances clés en matière de menaces. Nous terminerons par des suggestions qui devraient aider les utilisateurs à changer de comportement et à commencer à donner la priorité à la sécurité.

SOMMAIRE

Principales conclusions : monde

Plus de 1 million

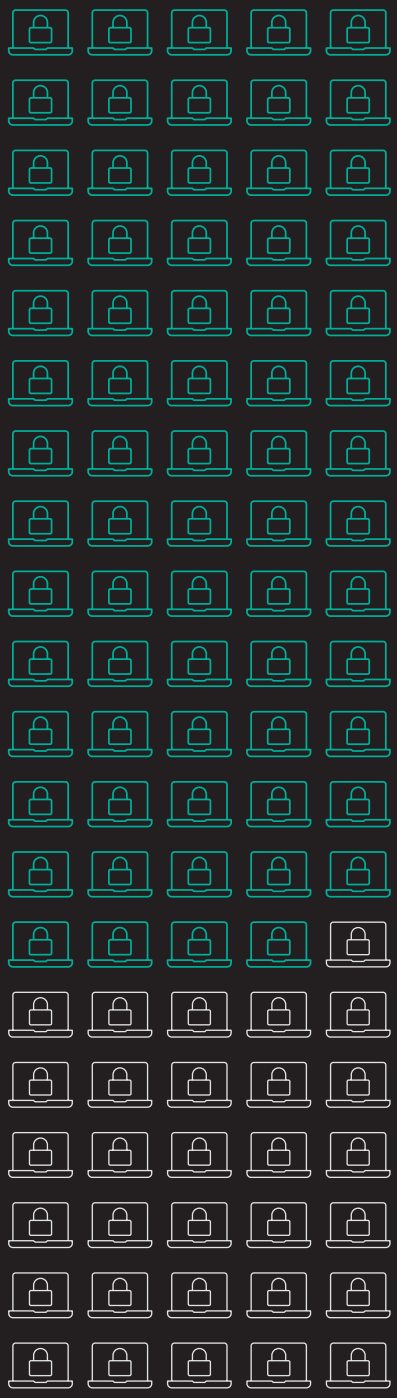
d'attaques sont lancées avec le framework de contournement de l'authentification multifacteur EvilProxy chaque mois, mais 89 % des professionnels de la sécurité pensent toujours que l'authentification multifacteur offre une protection totale contre la prise de contrôle de comptes.

des utilisateurs ont effectué une action dangereuse

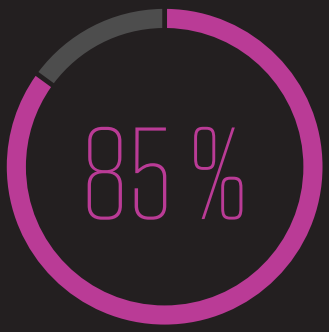
d'entre eux l'ont fait en sachant qu'ils prenaient un risque.

66 millions

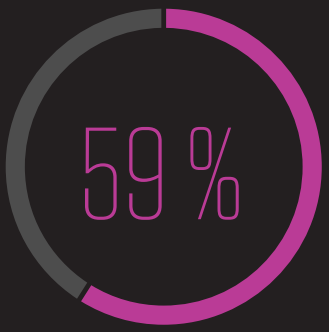
d'attaques BEC ont été détectées et bloquées en moyenne chaque mois par Proofpoint.



69 % des entreprises ont été infectées par des ransomwares.



des professionnels de la sécurité ont déclaré que la plupart des collaborateurs savent que la sécurité relève de leur responsabilité, mais



des utilisateurs ne le savaient pas ou ont indiqué qu'elle ne relevait pas du tout de leur responsabilité.

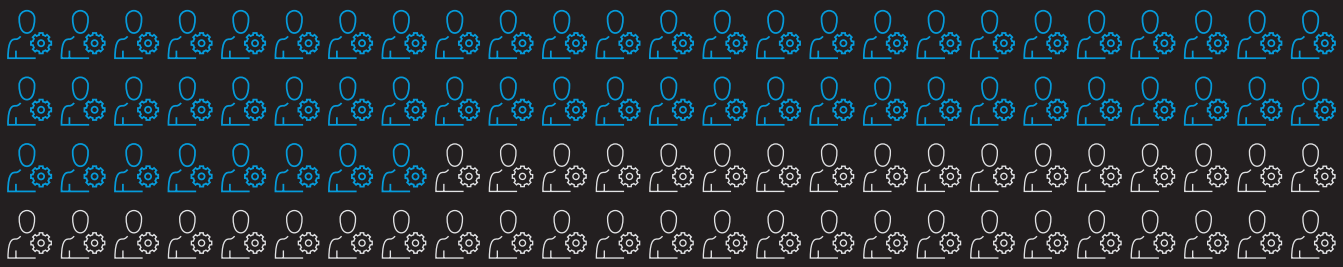
10 millions

de messages TOAD sont envoyés chaque mois.

Microsoft demeure la marque la plus usurpée, avec

68 millions

de messages malveillants associés à sa marque ou à ses produits.



58 %

des utilisateurs ayant effectué des actions dangereuses ont adopté un comportement qui les aurait rendus vulnérables aux tactiques d'ingénierie sociale courantes.

Zoom sur l'Europe et le Moyen-Orient

Pour les besoins du rapport State of the Phish 2024, nous avons interrogé 7 500 utilisateurs et 1 050 professionnels de la sécurité dans 15 pays. Cette synthèse se concentre sur les pays suivants :

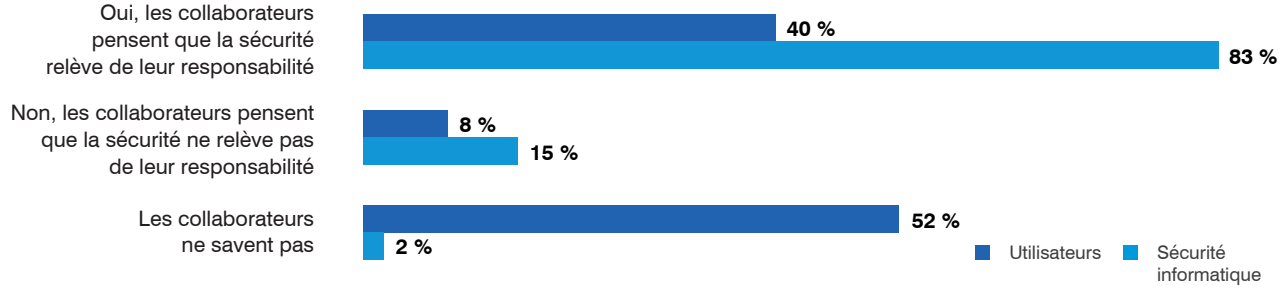
- France
- Allemagne
- Italie
- Pays-Bas
- Espagne
- Suède
- Royaume-Uni
- Émirats arabes unis

On observe d'importantes variations entre les régions et entre les huit pays concernés par cette synthèse, compte tenu de la diversité de leurs langues, cultures et niveaux de maturité numérique. La région est diversifiée sur les plans géographique, culturel et économique. Un aspect présente toutefois une certaine uniformité : les utilisateurs de la région ont été plus nombreux à admettre avoir effectué une action dangereuse que la moyenne mondiale (76 % contre 71 %). Pourtant, le pourcentage de personnes ayant déclaré qu'elles savaient que cette action comportait des risques était de 95 %, soit seulement un point de moins que la moyenne mondiale.

À l'échelle nationale, 86 % des sondés émiratis ont admis avoir effectué une action dangereuse, soit le pourcentage le plus élevé parmi tous les pays participant à l'enquête. Les entreprises émiraties ont également signalé le plus grand nombre d'attaques de spear phishing (harponnage) réussies, ce qui montre qu'il existe un lien étroit entre sensibilisation des utilisateurs et niveau de sécurité. Pourtant, les Émirats arabes unis ont enregistré le nombre le plus élevé d'utilisateurs considérant que la sécurité relève de leur responsabilité (62 % contre une moyenne mondiale de 41 %).

Les utilisateurs suédois ont été les moins nombreux à affirmer que la sécurité relève de leur responsabilité. Cela concorde avec le nombre supérieur à la moyenne d'utilisateurs effectuant des actions dangereuses (82 %) en Suède.

Responsabilité en matière de sécurité (Europe et Moyen-Orient)

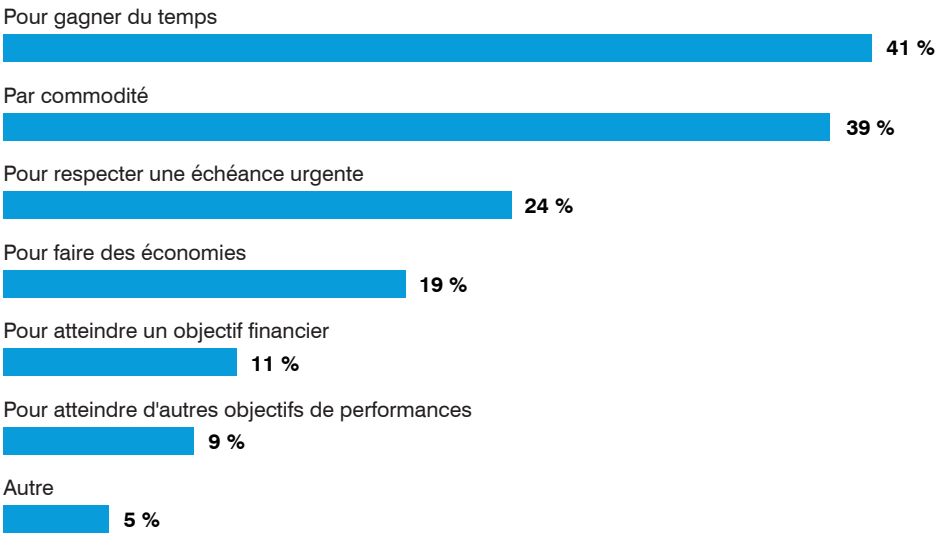


Les professionnels de la sécurité de la région ont cité la réutilisation de mots de passe comme le comportement le plus à risque. Malheureusement, le partage et la réutilisation de mots de passe sont le deuxième comportement le plus courant parmi les utilisateurs. Il y a tout de même une bonne nouvelle pour les équipes de sécurité : l'accès à des sites Web inappropriés est la seule autre action de leur top 5 à figurer également parmi les comportements les plus adoptés par les utilisateurs.

Classement	Comportements à risque (classés par les professionnels de la sécurité)	Comportements à risque (classés par les utilisateurs)
1	Réutilisation ou partage d'un mot de passe	Utilisation d'un terminal professionnel pour des activités d'ordre privé
2	Clic sur un lien ou téléchargement d'une pièce jointe provenant d'un inconnu	Réutilisation ou partage d'un mot de passe
3	Chargement de données sensibles sur un cloud tiers non approuvé	Connexion dans un lieu public sans utiliser de VPN
4	Divulgation d'identifiants de connexion à une source non fiable	Réponse à un message (email ou SMS) envoyé par un inconnu
5	Accès à un site Web inapproprié	Accès à un site Web inapproprié

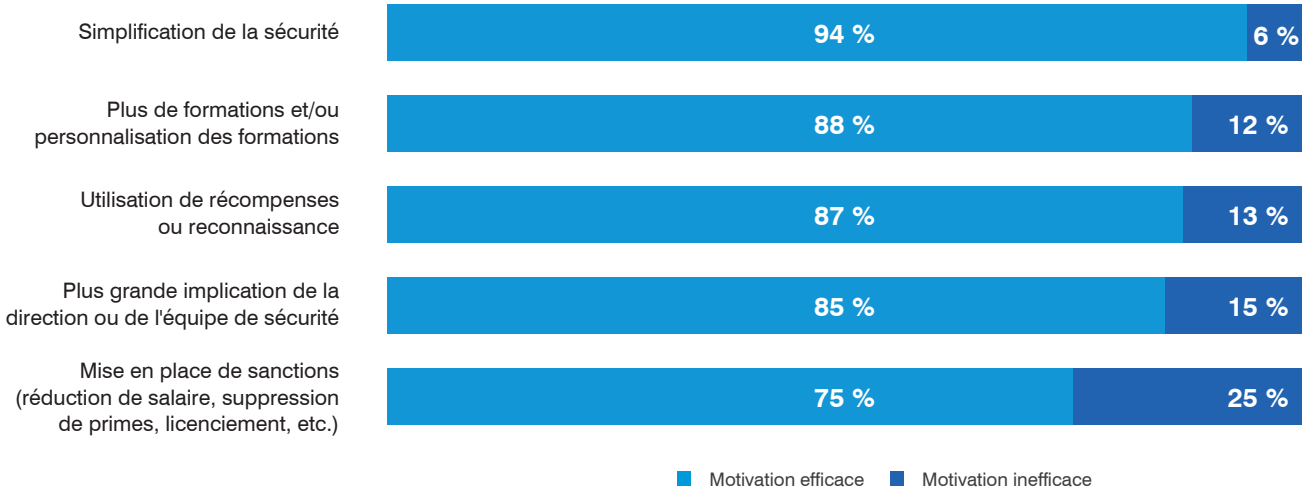
Mais pourquoi les utilisateurs effectuent-ils des actions dangereuses ? Le gain de temps a été la réponse la plus fréquente, suivi de près par la commodité. Au Royaume-Uni, la commodité arrive en première position et le gain de temps en deuxième, les sondés britanniques étant plus nombreux à citer la commodité que n'importe qui d'autre.

Raisons pour lesquelles les utilisateurs effectuent des actions dangereuses



Les utilisateurs en Europe et au Moyen-Orient expliquent clairement pourquoi ils effectuent des actions dangereuses. Mais comment pourraient-ils être encouragés à donner la priorité à la sécurité ? Comme à l'échelle mondiale, la plupart d'entre eux ont cité la simplification de la sécurité comme la motivation la plus efficace et les sanctions comme la motivation la moins efficace.

Stratégies pour motiver les utilisateurs à faire de la sécurité une priorité



78 %

des entreprises allemandes ont été victimes d'attaques TOAD, mais seulement

21 %

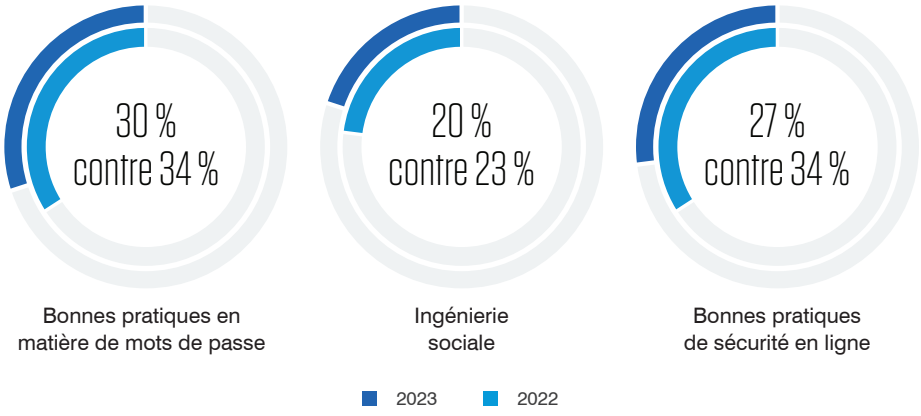
proposent des formations à ce sujet.

Possibilités d'amélioration

95 % des entreprises de la région utilisent déjà la threat intelligence pour élaborer leurs programmes de formation et de sensibilisation à la sécurité informatique. Cependant, on observe d'importantes lacunes. Alors que la plupart des entreprises ont déclaré avoir été ciblées par des attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery), moins d'un tiers d'entre elles les utilisent comme thème de formation. En Allemagne, 78 % des entreprises ont été victimes d'attaques TOAD, mais seulement 21 % d'entre elles proposent des formations à ce sujet, l'un des plus larges fossés entre attaques quotidiennes et thèmes de formation.

Globalement, le temps consacré aux formations de sensibilisation à la sécurité informatique a augmenté dans l'ensemble de la région. L'Espagne a connu la hausse la plus importante, avec une augmentation de 120 % du nombre d'entreprises consacrant trois heures ou plus par an à ces formations.

Toutefois, le pourcentage d'entreprises proposant des formations sur les thèmes essentiels suivants semble reculer :



Ce sont des thèmes de sécurité fondamentaux. Si moins d'utilisateurs savent comment configurer des mots de passe sécurisés, éviter les leurres courants et naviguer sur le Web en toute sécurité, les cybercriminels ne manqueront pas d'en profiter.

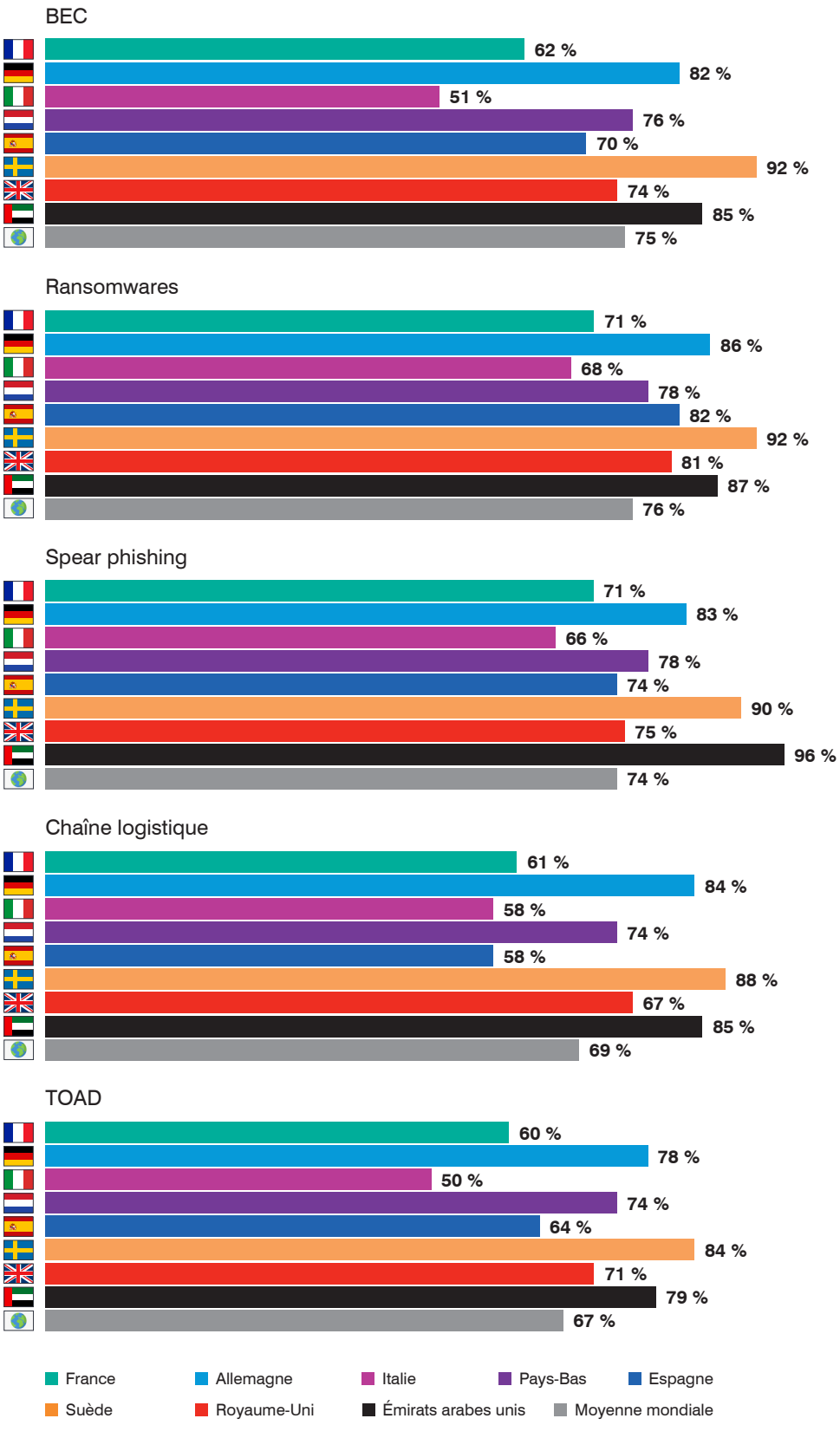
Paysage des menaces en Europe et au Moyen-Orient

L'année dernière, le paysage des menaces régional a largement suivi les tendances mondiales. Le piratage de la messagerie en entreprise (BEC, Business Email Compromise) a reculé au niveau mondial, mais une hausse de ces attaques a été constatée dans les pays non anglophones. Elle pourrait être liée à l'essor des outils d'IA générative tels que ChatGPT, qui peuvent être utilisés pour écrire des emails de leurre convaincants dans plusieurs langues. Des tendances similaires ont été observées dans d'autres pays non anglophones à travers le monde. Globalement, 75 % des entreprises ont été victimes d'au moins une attaque de phishing réussie, contre 88 % en 2022.

La région a été touchée par un nombre légèrement plus important d'attaques TOAD — 70 %, contre une moyenne mondiale de 67 %. 84 % des entreprises suédoises ont subi une attaque TOAD, soit le pourcentage le plus élevé dans la région.

Tout comme à l'échelle mondiale, les entreprises en Europe et au Moyen-Orient ont fait état d'une augmentation des conséquences négatives découlant d'attaques réussies. Les sanctions financières ont bondi de 122 %, un pourcentage légèrement inférieur à la moyenne mondiale, ce qui pourrait indiquer que des amendes au titre du RGPD auraient déjà été payées au cours des années précédentes.

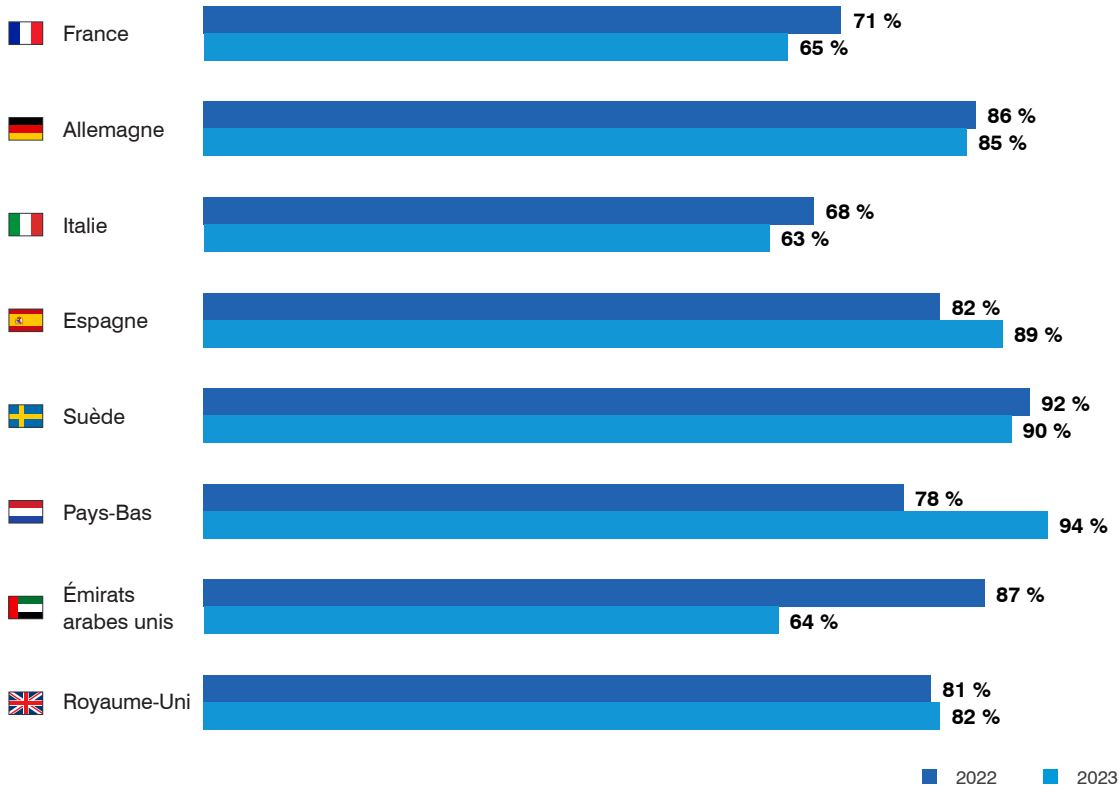
Pourcentage d'entreprises visées par des attaques ciblées



Ransomwares

Les ransomwares demeurent une menace grave pour les entreprises de la région. Tant les attaques que les infections ont augmenté au cours de l'année écoulée. Toutefois, les détails varient en fonction du pays.

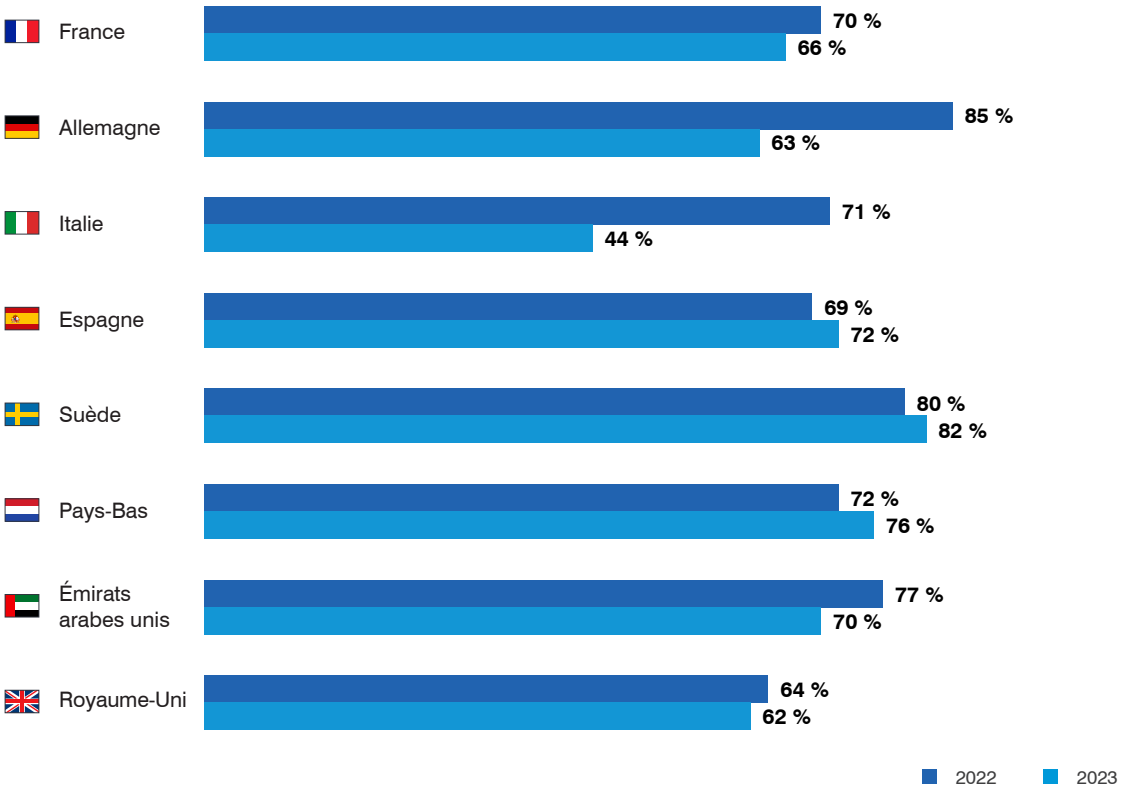
Attaques de ransomwares par email – Tendance



Par exemple, ce sont les entreprises italiennes qui ont enregistré la plus importante hausse du nombre d'infections de ransomwares réussies, passant de 44 % en 2022 à 71 % en 2023, alors qu'elles font face au même volume d'attaques que les entreprises des autres pays. Cela a poussé les autorités italiennes à lancer un avertissement au mois de juin concernant le nombre croissant d'attaques de ransomwares exploitant un bug VMware.

La Suède a quant à elle enregistré le pourcentage le plus élevé au monde de tentatives d'attaques de ransomwares, 92 % de ses entreprises ayant été ciblées. Cela pourrait être lié au fait que, lors d'une enquête précédente, 74 % des sondés suédois ont cité le vol d'identifiants de connexion comme la principale cause de compromissions de données. Le fait de prioriser la défense contre ces attaques pourrait réduire la probabilité d'activités secondaires, telles que le déploiement d'un ransomware.

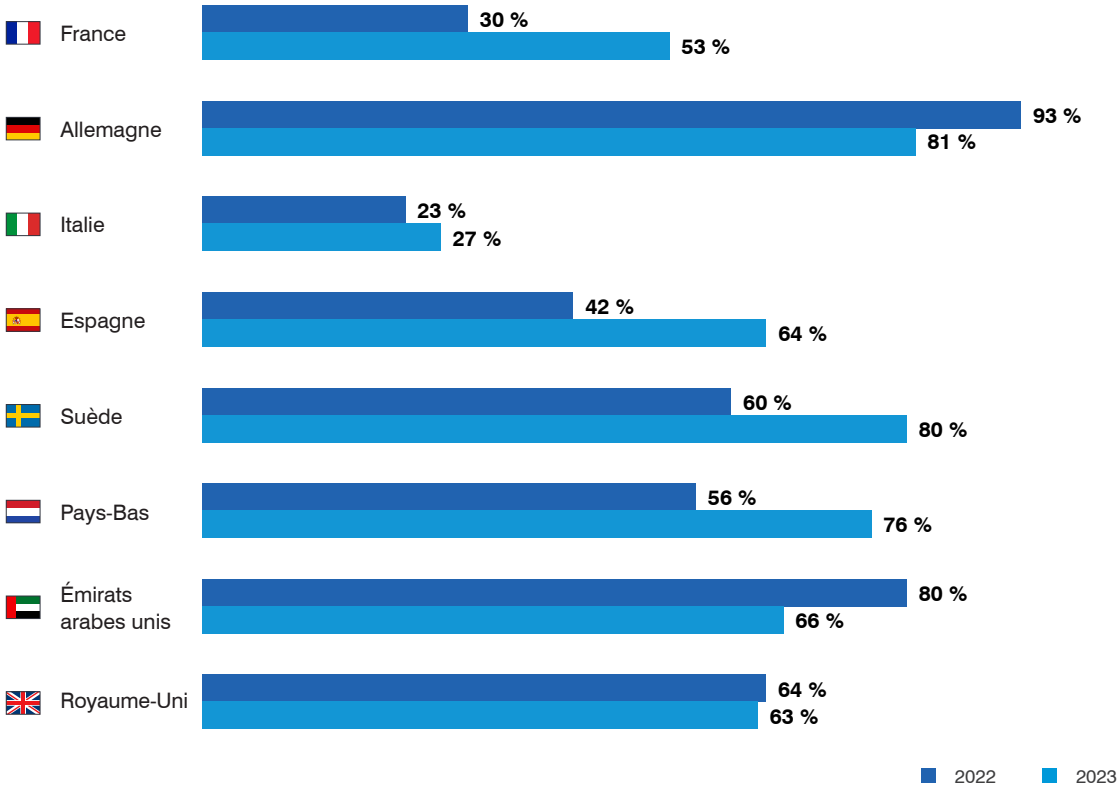
Infections de ransomwares – Tendance



Par ailleurs, seuls trois pays — l'Allemagne, les Émirats arabes unis et le Royaume-Uni — ont démontré une plus grande volonté à payer. C'est en Allemagne que le pourcentage d'entreprises ayant payé une rançon est également le plus élevé (93 %, contre une moyenne mondiale de 54 %).

Cette stratégie a semblé fonctionner pour les entreprises allemandes et émiraties, qui ont été bien plus nombreuses à récupérer leurs systèmes et données après un seul paiement. Le fait que 85 % des entreprises allemandes aient déclaré avoir été victimes d'une infection de ransomware réussie, le pourcentage le plus élevé de la région, suggère un lien entre leur disposition à payer et l'intensité de ciblage.

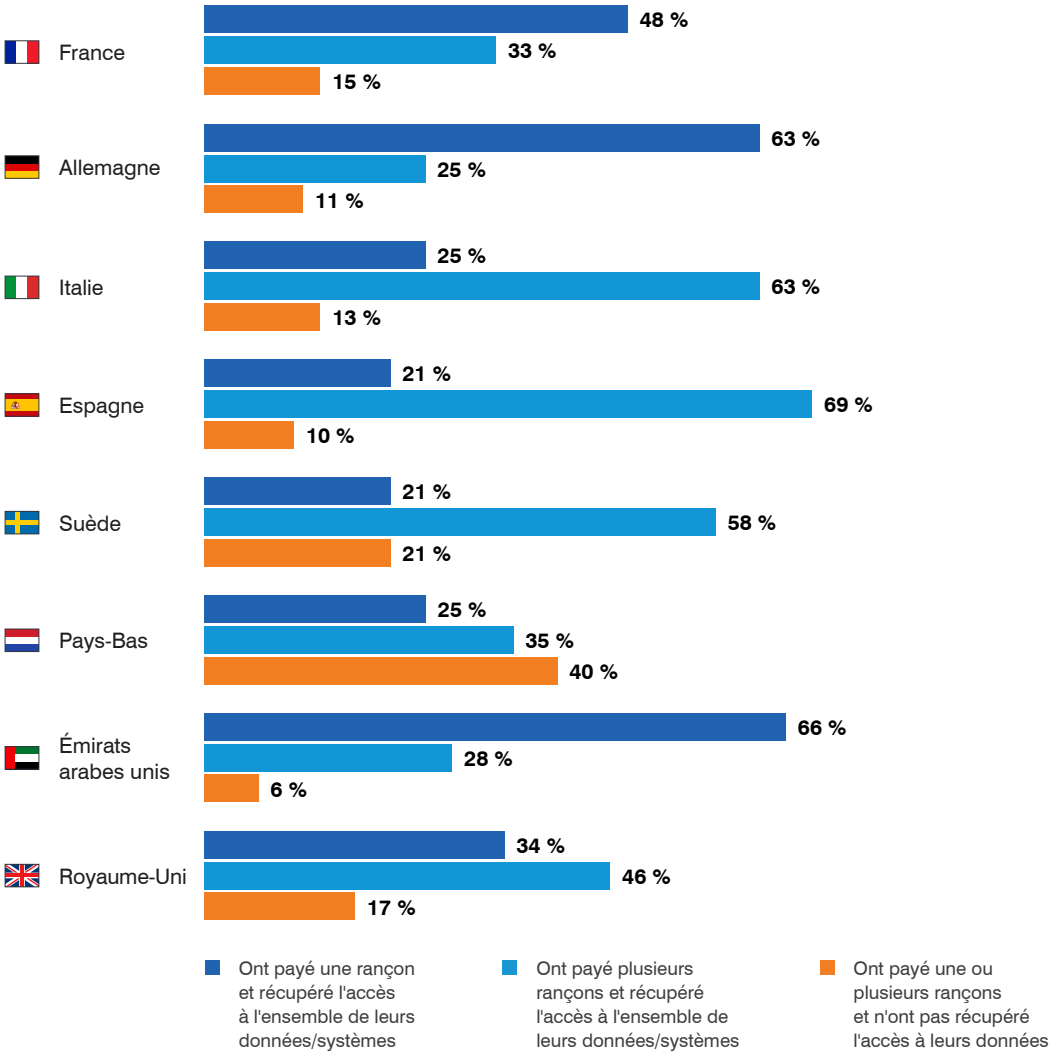
Pourcentage d'entreprises ayant payé une rançon



Les entreprises britanniques ne s'en sont pas aussi bien sorties. En effet, elles ont enregistré le pourcentage le plus élevé d'infections répétées. Près de 14 % d'entre elles ont subi 10 infections ou plus, contre une moyenne mondiale de 5 %. Cela montre que le paiement de rançons ne garantit pas une immunité contre les attaques futures, et pourrait même les encourager.

Les entreprises néerlandaises sont celles qui ont observé le moins de résultats positifs suite à un paiement. 40 % d'entre elles ont déclaré ne jamais avoir récupéré leurs données, contre 16 % à l'échelle mondiale. Cela suggère que certains groupes de ransomwares peuvent ne pas honorer leurs promesses ou ne pas toujours être en capacité de restaurer les données.

Résultats suite au paiement d'une rançon



Sur une note positive, les niveaux de couverture par les contrats de cyberassurance se sont améliorés, offrant un certain soulagement financier. La France fait figure d'exception. Le pourcentage d'entreprises partiellement ou entièrement couvertes est passé de 87 % en 2022 à 76 % en 2023. Cela est probablement dû au fait que la plus grande compagnie d'assurance française a annoncé qu'elle ne couvrirait plus les attaques de ransomwares.

Recommandations

Les résultats de notre enquête montrent que les utilisateurs en Europe et au Moyen-Orient comprennent que leur comportement comporte des risques. Toutefois, cela ne suffit souvent pas à les convaincre d'accorder la priorité à la sécurité. Certains privilégient la commodité ou veulent gagner du temps, tandis que d'autres ne savent tout simplement pas si la sécurité informatique relève de leur responsabilité.

Pour les utilisateurs qui ont déjà compris que la sécurité relève de leur responsabilité

- Fournissez aux utilisateurs des outils leur permettant d'être plus proactifs. Les boutons de signalement d'emails permettent de signaler facilement les messages suspects. Par ailleurs, les technologies d'encouragement, telles que l'affichage d'avertissements en cas d'emails suspects, peuvent inciter les utilisateurs à agir. Envisagez également de mettre en place un réseau de promoteurs et un système de récompenses pour encourager ces utilisateurs à modéliser les bonnes pratiques et à devenir les défenseurs du signalement auprès de leurs collègues qui ne savent pas comment s'y prendre.

Pour les utilisateurs qui ne savent pas ou qui pensent que la sécurité ne relève pas de leur responsabilité

- Proposez des formations personnalisées et pertinentes pour chaque rôle et ses responsabilités. Multipliez les communications de la direction et des responsables de la sécurité pour mieux informer les utilisateurs de leurs responsabilités et de leur impact sur l'entreprise.

Il est également important de proposer des formations à la sécurité informatique ainsi que des fonctionnalités de prévention, de détection et de réponse de premier ordre. Des solutions avancées peuvent contribuer à trouver le juste équilibre entre contrôles de sécurité plus stricts et productivité, en réduisant le nombre de menaces auxquelles sont confrontés les utilisateurs. Par exemple, le déploiement d'une solution de protection de la messagerie électronique efficace à 99,9 % signifie que la plupart des utilisateurs n'auront jamais à décider de la façon dont réagir face à un lien suspect.

Enfin, collaborez avec les parties prenantes de l'entreprise et privilégiez la facilité d'utilisation lors de l'implémentation de règles de sécurité. Les utilisateurs seront moins enclins à contourner les systèmes si la sécurité s'aligne sur leurs objectifs. Et ils seront plus susceptibles d'utiliser un contrôle s'il est intuitif et ne requiert aucune formation.

EN SAVOIR PLUS

Pour découvrir comment Proofpoint peut vous fournir des informations sur les risques liés aux utilisateurs et vous aider à les limiter grâce à une stratégie de cybersécurité centrée sur les personnes, consultez le site **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0402-001-03-01