proofpoint.

RAPPORT

Europe et Moyen-Orient

2023 State of the Phish

Sensibilisation des utilisateurs, vulnérabilités et résilience – Analyse approfondie

proofpoint.com/fr

UNE ENQUÊTE MENÉE AUPRÈS DE :

7 500

adultes actifs dans 15 pays

1 050

professionnels de la sécurité informatique de ces mêmes pays

ET S'APPUYANT SUR :

135 millions

de simulations d'attaques de phishing envoyées par nos clients sur une période de 12 mois

18 millions

d'emails signalés par les utilisateurs de nos clients sur une période de 12 mois

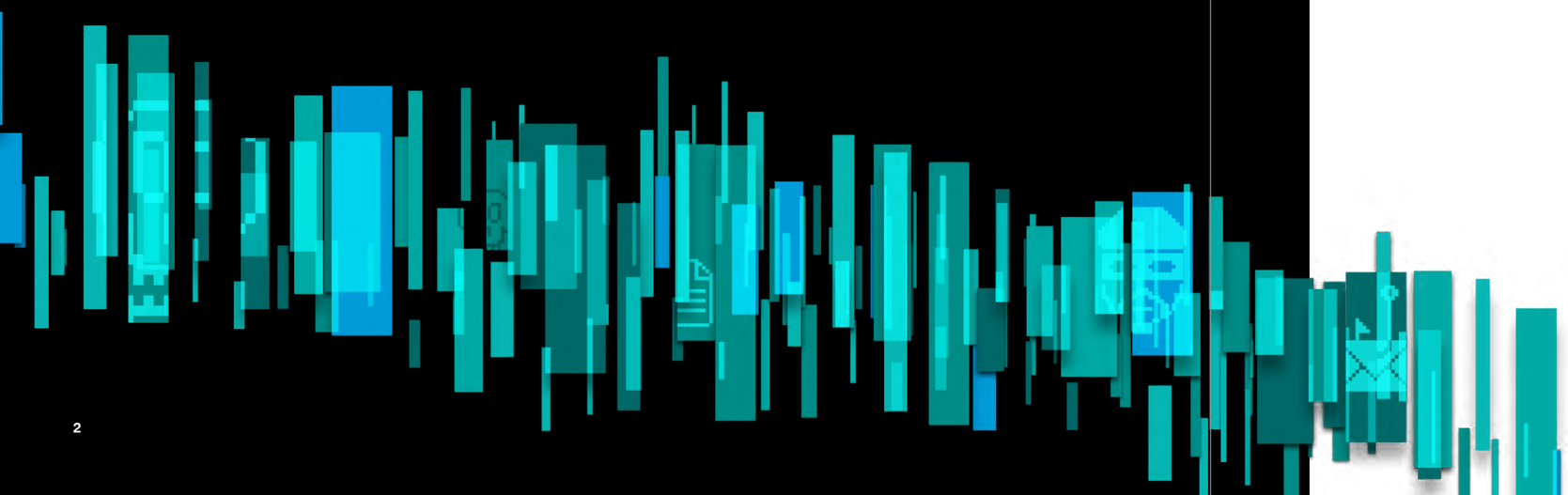
2022 : une année placée sous le signe de la créativité pour les cybercriminels

Chaque année, les cybercriminels mettent au point de nouveaux stratagèmes pour tromper leurs victimes et contourner les défenses. 2022 n'a pas fait exception. Les entreprises ont déployé de nouveaux contrôles de sécurité, auxquels les cybercriminels se sont adaptés.

Les cybercriminels ont ajouté à leur arsenal des techniques complexes comme les attaques par téléphone et le contournement de l'authentification multifacteur (MFA). Inconnues de la plupart des utilisateurs, ces techniques ont procuré aux cybercriminels un avantage inédit. Face à une telle répartie, les RSSI et les équipes de sécurité des informations n'ont pas manqué de travail.

Notre neuvième rapport annuel *State of the Phish* s'appuie sur les données recueillies dans le cadre d'une enquête menée dans 15 pays pour évaluer la sensibilisation des utilisateurs, les vulnérabilités et la résilience. Le rapport compare le degré de compréhension des cyberattaques et des tactiques de défense courantes. Il analyse également comment le manque de connaissances et les mauvaises pratiques en matière de cybersécurité favorisent le développement du paysage des menaces. La plupart des attaques ciblent les personnes avant de viser les systèmes. C'est la raison pour laquelle la dernière section de ce rapport s'intéresse aux pratiques en matière de formation à la sécurité et met l'accent sur les possibilités d'instaurer et de maintenir une culture de la sécurité informatique à tous les niveaux.

En plus du rapport principal, nous avons élaboré des synthèses régionales afin de déterminer comment les nuances locales affectent les lacunes en matière de sensibilisation. Cette synthèse régionale inclut des données **d'Allemagne, de France, d'Espagne, d'Italie, des Pays-Bas, du Royaume-Uni, de Suède et des Émirats arabes unis**. Ces données sont issues d'une enquête réalisée auprès de 4 000 adultes actifs et de 650 professionnels de la sécurité informatiques.



SOMMAIRE

Principales conclusions à l'échelle mondiale

44 %

des sondés pensent qu'un email est sûr lorsqu'il contient une marque familière

600 000 par jour

300 000-400 000

tentatives d'attaques par téléphone ont eu lieu chaque jour en 2022, avec un pic à 600 000 par jour en août

1/3

des sondés ont effectué une action dangereuse (comme cliquer sur un lien ou télécharger un malware) lors d'une attaque

76 %

Augmentation des pertes financières directes liées aux attaques de phishing fructueuses

30 millions

de messages malveillants envoyés en 2022 impliquaient la marque ou des produits Microsoft

> 1 sur 10

Proportion de menaces bloquées suite au signalement d'un utilisateur

> 1/3

des sondés ne savent pas définir les termes « malware », « phishing » et « ransomware »

Même des concepts de base ne sont pas compris

SEULEMENT 35 %

des entreprises exécutent des simulations de phishing

64 % des entreprises infectées par un ransomware ont payé une rançon

90 % des entreprises victimes d'un ransomware avaient souscrit un contrat de cyberassurance

65 % des entreprises ont signalé au moins une fuite de données d'origine interne

SEULEMENT 56 %

des entreprises ayant mis en place un programme de sensibilisation à la sécurité informatique forment tous leurs collaborateurs

90 %

des professionnels de la sécurité considèrent la sécurité comme une priorité absolue dans leur entreprise

mais

33 %

des collaborateurs admettent que la cybersécurité ne fait pas partie de leurs priorités au travail

94 %

des entreprises suédoises ont subi une attaque de phishing fructueuse

mais…

Seulement 18 %

des entreprises suédoises forment les utilisateurs qu'elles savent ciblés

Zoom sur l'Europe et le Moyen-Orient

On observe d'importantes variations entre les 15 pays sondés pour les besoins du rapport *State of the Phish*, ce qui n'a rien de surprenant compte tenu de la diversité de leurs langues, cultures et niveaux de maturité numérique. Le même constat est applicable aux huit pays concernés par cette synthèse.

Parmi toutes les régions sondées, l'EMEA, qui comprend l'Europe, le Moyen-Orient et l'Afrique, est sans doute la plus diversifiée. Cet immense territoire géographique, qui couvre à la fois l'hémisphère nord et l'hémisphère sud, présente des cultures, des politiques et des économies radicalement différentes. Comme de nombreux lieux en 2022, les pays de la région EMEA ont été le théâtre de changements géopolitiques et de l'aggravation des conflits. Sans surprise, cela s'est reflété dans le paysage de la cybersécurité.

Avec 94 %, les entreprises suédoises ont été les plus nombreuses à subir une attaque de phishing fructueuse parmi tous les pays sondés. Naturellement, plusieurs facteurs peuvent être à l'origine des données hors norme. Celles-ci pourraient notamment s'expliquer par la faible importance accordée aux formations de sensibilisation à la sécurité informatique dans le pays. En effet, seulement 18 % des entreprises suédoises forment les utilisateurs qu'elles savent ciblés, soit le pourcentage le plus faible parmi les pays sondés. Il est également possible que les taux de signalement soient plus élevés. La Suède est une pionnière de la sécurité des données depuis les années 1970, et a adopté l'une des premières lois européennes sur la protection de la vie privée numérique. Il y est donc peut-être plus acceptable sur le plan culturel d'admettre des compromissions de sécurité, ce qui se traduit par un signalement plus précis.

Cette année, nous avons pour la première fois inclus l'Italie, et les résultats sont étonnants. Parmi les 15 pays sondés, les entreprises italiennes ont été les moins nombreuses à être visées par un large éventail de types de menaces. Seulement 47 % d'entre elles ont perdu des données ou des éléments de propriété intellectuelle en raison d'une attaque externe (contre une moyenne mondiale de 69 %). Par rapport aux autres pays sondés, les entreprises italiennes ont été les moins nombreuses à subir une attaque de phishing fructueuse (79 %). Ces chiffres peuvent indiquer un décalage ou une immaturité concernant les réglementations relatives au signalement des incidents de sécurité. Ils peuvent aussi être le reflet d'une culture moins centrée sur la transparence des informations.

Si l'on s'intéresse à d'autres catégories de cyberattaques, on constate que le piratage de la messagerie en entreprise (BEC, Business Email Compromise) se répand à la vitesse grand V. Les Pays-Bas et la Suède ont enregistré le taux d'attaques le plus élevé avec 92 % (contre une moyenne mondiale de 75 %). C'est en Allemagne et en Espagne que le nombre d'incidents a augmenté le plus rapidement, de 16,5 % en moyenne par rapport à l'année précédente. L'évolution de la langue peut également jouer un rôle déterminant dans la multiplication des attaques BEC. Auparavant, la grande majorité des emails BEC étaient écrits en anglais. Mais récemment, nous avons constaté une augmentation des emails BEC rédigés en allemand, en espagnol, en slovène et dans d'autres langues. Cela concorde avec la sophistication croissante des attaques.

Les Pays-Bas étaient le pays le plus ciblé par des cyberattaques menées par des utilisateurs internes (86 % contre une moyenne mondiale de 66 %) et des cybercriminels externes (84 % contre une moyenne mondiale de 68 %). Mais les formations semblent efficaces. Les collaborateurs néerlandais ont été les moins nombreux à divulguer leurs informations personnelles ou leurs mots de passe.

PARLONS TERMINOLOGIE :

Même des concepts de base ne sont toujours pas compris correctement. En effet, plus d'un tiers des sondés ne savent pas définir les termes « malware », « phishing » et « ransomware ».

40 %

des utilisateurs savent ce qu'est un ransomware, soit 9 points de plus qu'en 2019 — la plus forte augmentation parmi les termes mentionnés

29 et 30 %

des utilisateurs connaissaient les termes relativement récents « SMiShing » et « vishing », respectivement

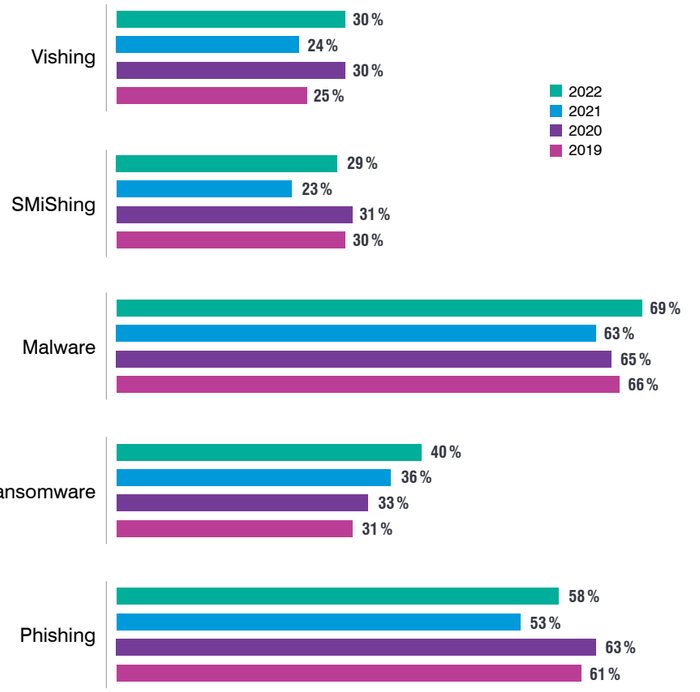
58 %

des utilisateurs savent ce qu'est le phishing, soit 5 points de plus que l'année précédente, mais 3 points de moins qu'en 2019

Sensibilisation à la sécurité : chiffres et opportunités

Parmi les 15 pays sondés, une tendance similaire se dessine en ce qui concerne la connaissance qu'ont les utilisateurs des termes de sécurité de base. Les menaces courantes telles que le phishing, les ransomwares et les malwares sèment le chaos depuis des années, mais les utilisateurs ne comprennent toujours pas bien ce qu'elles représentent. Les menaces plus récentes comme le SMiShing (phishing par SMS) et le vishing (phishing vocal) sont encore moins comprises. Malheureusement, nos données montrent peu d'évolution par rapport à l'année précédente.

La compréhension des utilisateurs a peu évolué par rapport à l'année précédente



LE PRINCIPE D'INCERTITUDE :

69 %

des utilisateurs néerlandais savaient ce qu'est le phishing, soit le pourcentage le plus élevé parmi les huit pays sondés dans cette région

45 %

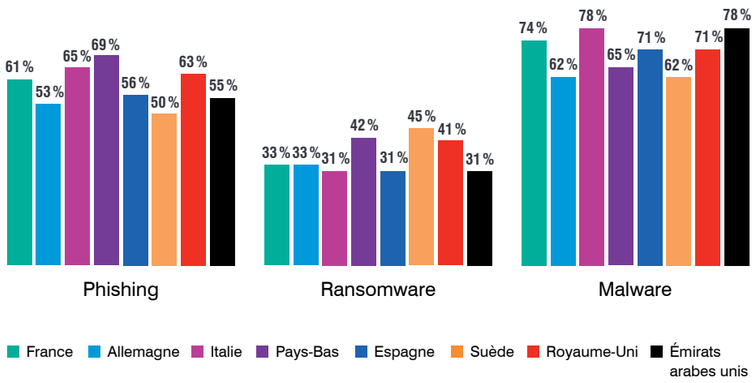
des utilisateurs suédois savaient définir un ransomware, devançant les sept autres pays

78 %

des utilisateurs italiens et émiratis savaient ce qu'est un malware, soit le pourcentage le plus élevé parmi les huit pays sondés dans cette région

Plusieurs différences notables émergent lorsque l'on compare la connaissance qu'ont les utilisateurs des trois menaces les plus courantes. Les sondés suédois et allemands ont été les moins nombreux à savoir définir les termes « malware » et « phishing ». Les sondés émiratis et italiens ont été les plus nombreux à savoir définir le terme « malware », mais ont obtenu des résultats inférieurs à la moyenne pour le terme « ransomware ».

Connaissance des menaces courantes (précision)



Ces différences peuvent s'expliquer par le fait que moins de 50 % des entreprises d'Europe et du Moyen-Orient proposent des formations sur ces thématiques. Les moyennes régionales étaient de 37 % pour le phishing, 34 % pour les ransomwares, 40 % pour les malwares et 27 % pour les attaques BEC.

FORMATIONS THÉMATIQUES :

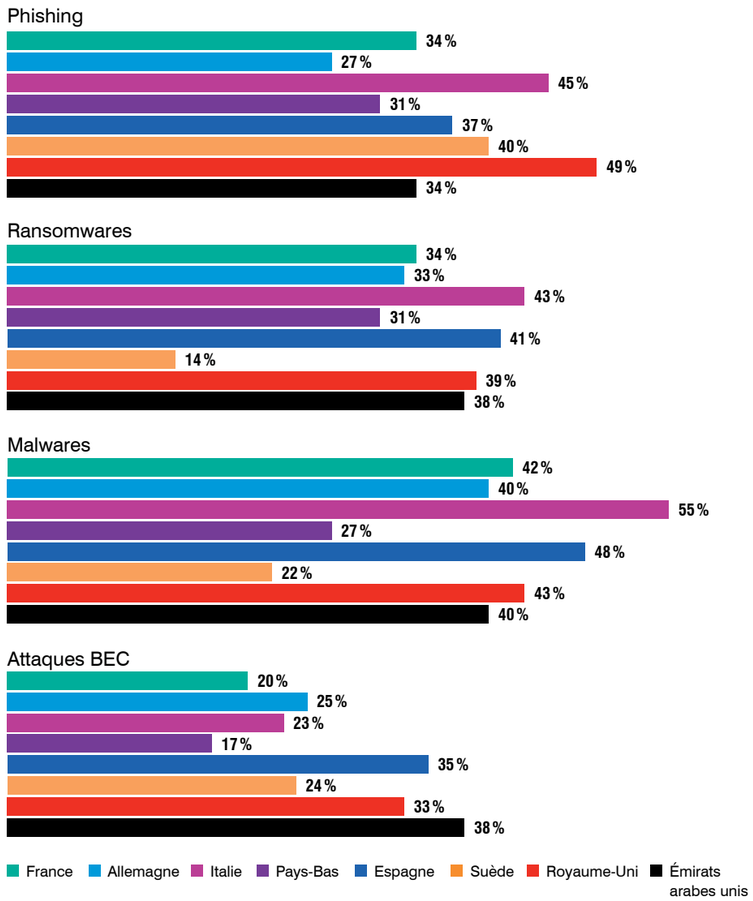
55 %

des entreprises italiennes apprennent à leurs utilisateurs à identifier les malwares, soit le pourcentage le plus élevé enregistré pour une thématique dans l'ensemble des pays de cette région

14 %

des entreprises suédoises apprennent à leurs utilisateurs à identifier les ransomwares, soit le pourcentage le plus faible enregistré pour une thématique dans l'ensemble des pays de cette région

Thématiques abordées dans les programmes de formation et de sensibilisation à la sécurité



Si la plupart des entreprises ont mis en place un programme de sensibilisation à la sécurité informatique, tous les collaborateurs ne suivent pas une formation pour autant. Les entreprises émiraties font figure d'exception : 64 % d'entre elles forment tous leurs collaborateurs et 52 % forment les utilisateurs qu'elles savent ciblés. Par ailleurs, 74 % des entreprises émiraties proposent à leurs collaborateurs des formations sur des thématiques de sécurité qui les ciblent explicitement, soit un pourcentage plus élevé que dans les 14 autres pays sondés.

SENSIBILISATION POUR TOUS :

64 %

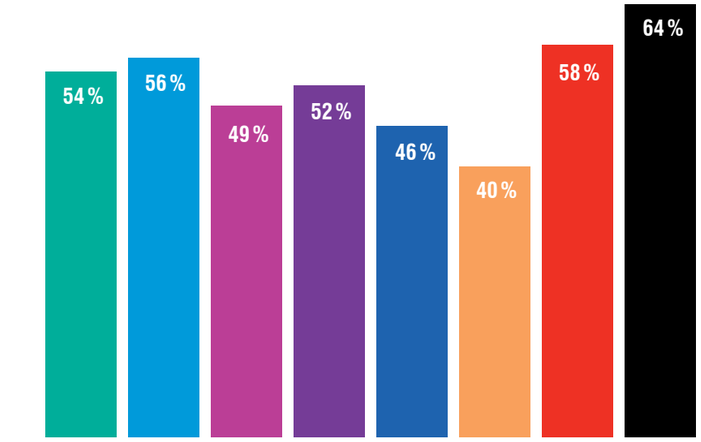
des employeurs émiratis ont formé tous les collaborateurs de leur entreprise, soit le pourcentage le plus élevé parmi les pays sondés en Europe et au Moyen-Orient

40 %

des entreprises suédoises ont fait de même, soit le pourcentage le plus faible parmi les pays sondés dans cette région

Les RSSI britanniques semblent réussir à faire de la sécurité informatique une priorité dans leur entreprise. Les collaborateurs britanniques étaient les plus enclins à avoir confiance en leur équipe informatique et à affirmer que leur entreprise fait de la cybersécurité une priorité. Cette croyance peut être due à la formation. En effet, les entreprises britanniques et émiraties ont enregistré le pourcentage le plus élevé de formation des utilisateurs qu'elles savent ciblés (52 %).

Pourcentage d'entreprises formant tous leurs collaborateurs dans le cadre de leur programme de sensibilisation à la sécurité informatique



Avec 48 %, les entreprises espagnoles ont été les plus nombreuses à exécuter des simulations d'attaques de phishing (voir les graphiques sur la page suivante). Le Royaume-Uni s'est démarqué en accordant une importance particulière au contact personnel, avec 45 % de formations en personne. Dans la région, les entreprises britanniques ont été les plus nombreuses à aborder le phishing (49 %), mais nettement moins nombreuses à exécuter des simulations de phishing (39 %) que les entreprises espagnoles.

TYPES DE FORMATION :

45 %

des entreprises britanniques ont proposé une formation en personne, soit le pourcentage le plus élevé parmi les pays sondés en Europe et au Moyen-Orient

50 et 48 %

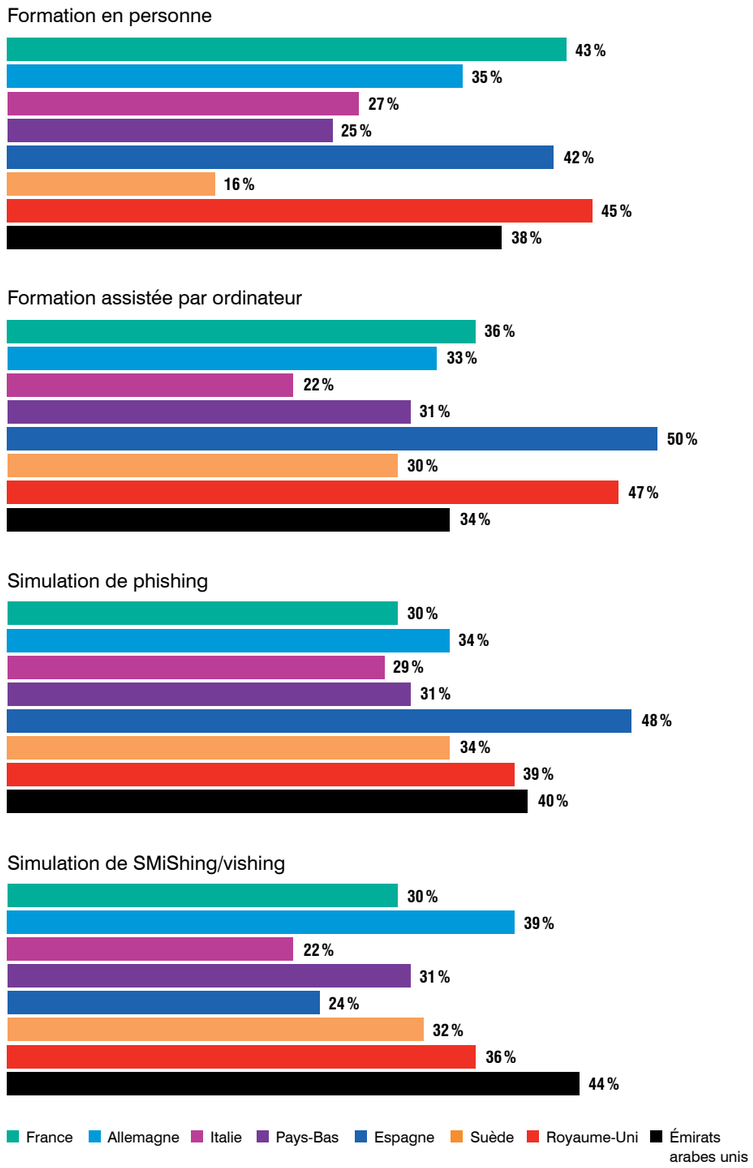
des entreprises espagnoles ont proposé une formation assistée par ordinateur et ont exécuté des simulations d'attaques de phishing, respectivement, ce qui les distingue des autres pays

44 %

des entreprises émiraties ont exécuté des simulations de SMiShing et de vishing, soit le pourcentage le plus élevé dans cette région

Les chiffres concernant les entreprises suédoises laissent penser qu'elles ne prennent pas la sécurité informatique suffisamment au sérieux. Peu d'entreprises proposent des formations en personne (16 %). Les entreprises suédoises sont également les moins nombreuses à former tous leurs collaborateurs (40 %). Ces chiffres sont étonnants, car les infections de ransomwares sont plus fréquentes en Suède que dans n'importe quel autre pays sondé (82 %).

Types de formation



LA MENACE QUI VIENT DE L'INTÉRIEUR :

71 %

des entreprises de la région EMEA ont perdu des données en raison d'incidents d'origine interne

54 %

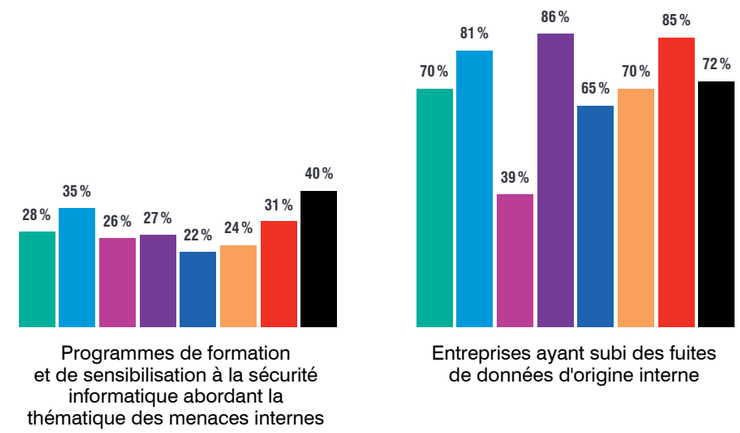
ont été victimes de trois attaques ou plus

Sensibilisation à la sécurité : menaces internes

Cette année, nous avons élargi notre enquête afin de refléter l'influence croissante des menaces internes, une catégorie qui englobe à la fois le vol de données par des utilisateurs malveillants, les fuites de données dues à la négligence des collaborateurs et le vol d'identifiants de connexion.

Dans toute la région, 71 % des entreprises en moyenne ont perdu des données en raison d'incidents d'origine interne. Il convient de noter le décalage entre le volume élevé d'attaques et la faible importance accordée aux formations de sensibilisation à la sécurité informatique (29 %).

Risques internes de fuite de données



Les entreprises allemandes ont été les plus nombreuses à subir des attaques fréquentes d'origine interne (18 %), et les collaborateurs allemands ont été les plus nombreux à emporter avec eux des informations professionnelles à leur départ. C'est peut-être parce que les collaborateurs allemands pensent que ces informations leur appartiennent — seulement 35 % des entreprises allemandes proposent des formations sur les menaces internes. Si l'on compare avec les entreprises émiraties, bien que seulement 4 % d'entre elles signalent des attaques fréquentes d'origine interne, elles sont 40 % à former leurs collaborateurs. Cela s'explique peut-être par le fait que les collaborateurs émiratis ont été les plus nombreux de la région (29 %) à divulguer accidentellement des informations personnelles ou des mots de passe à des personnes en qui ils ne devraient pas avoir confiance.

VACANCES ROMAINES :

Les entreprises italiennes ont été moins nombreuses que celles des autres pays sondés à subir des attaques ciblées de différents types.

79 %

ont été victimes d'attaques de phishing

51 %

ont été visées par des attaques BEC

63 %

ont été ciblées par des ransomwares (seuls les Émirats arabes unis ont enregistré un pourcentage inférieur)

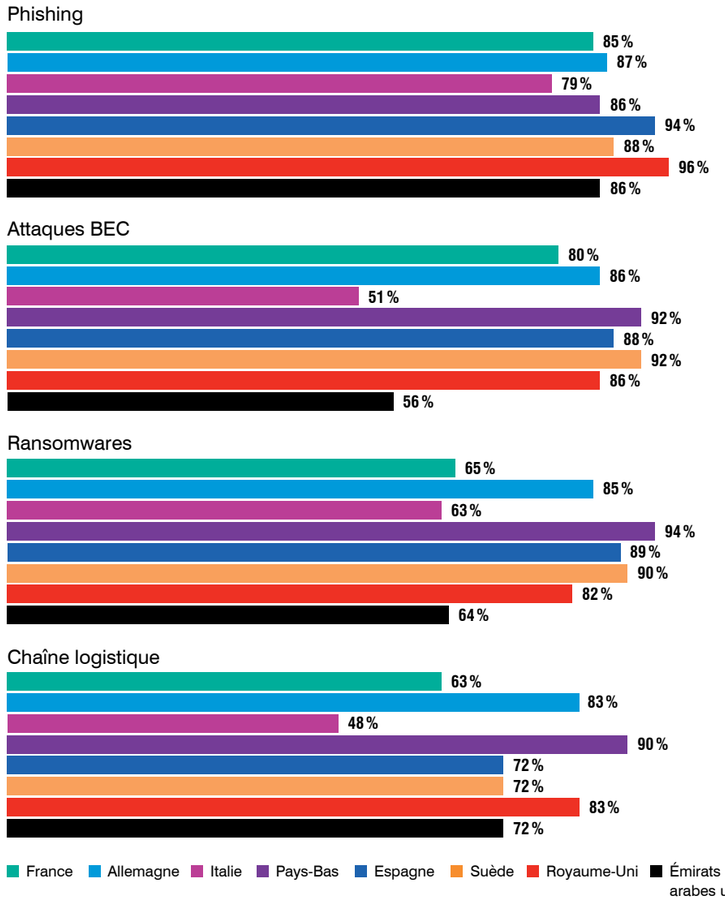
48 %

ont subi des attaques de la chaîne logistique

Tendances du paysage des menaces

Globalement, les entreprises françaises se démarquent en se situant dans la médiane de la région pour tous les types d'attaques ciblées. Nous pensons que ces chiffres reflètent le niveau de maturité du pays en matière de cybersécurité.

Pourcentage d'entreprises visées par des attaques ciblées



PAIEMENT DE RANÇONS :

27 %

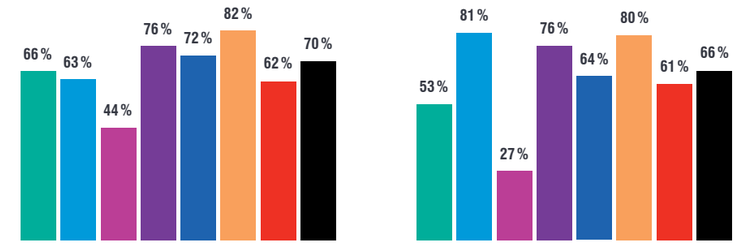
des entreprises italiennes infectées par un ransomware ont payé la rançon exigée par les cybercriminels, soit le pourcentage le plus faible parmi les pays sondés. Les entreprises italiennes ont également été les moins nombreuses à être infectées (44 %) et à être indemnisées par leur assureur (56 %).

Ransomwares : les assurances prêtent main-forte aux victimes

Les ransomwares sont déployés dans un second temps, après la compromission initiale. Cinq pays de la région EMEA ont démontré une forte probabilité d'infection de ransomware.

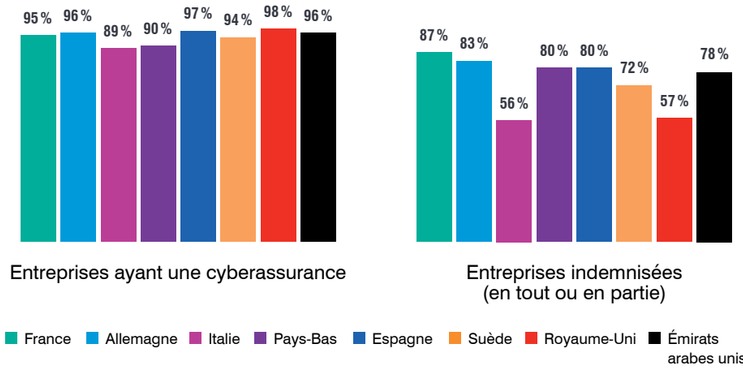
Parmi tous les pays sondés, les entreprises suédoises ont été les plus nombreuses à être infectées par un ransomware (82 %). La Suède fait partie des pays les mieux connectés au monde. Elle est une pionnière de la numérisation du secteur public et des principaux secteurs d'activité. Ces chiffres peuvent s'expliquer par le fait que pendant la pandémie, de nombreuses entreprises ont négligé leur protection contre les cybermenaces.

Infections de ransomwares et paiements



Alors que les entreprises allemandes ont été les plus nombreuses à payer la rançon (81 % contre une moyenne mondiale de 64 %), les entreprises britanniques ont globalement davantage souffert que les 14 autres pays. Non seulement elles n'ont pas récupéré l'accès à leurs données suite au paiement (33 % contre 52 %), mais leurs demandes d'indemnisation ont été refusées dans la plupart des cas (23 % contre 7 %).

Infections de ransomwares et paiements



Recommandations

Compte tenu des importantes variations entre les marchés et les entreprises, l'idéal est d'élaborer un programme de sécurité individuel tenant compte des menaces réelles et des risques liés aux utilisateurs. Si vous n'en êtes pas encore là, le rapport State of the Phish 2023 recommande quelques approches utiles.

Réduisez la complexité en posant les bonnes questions.

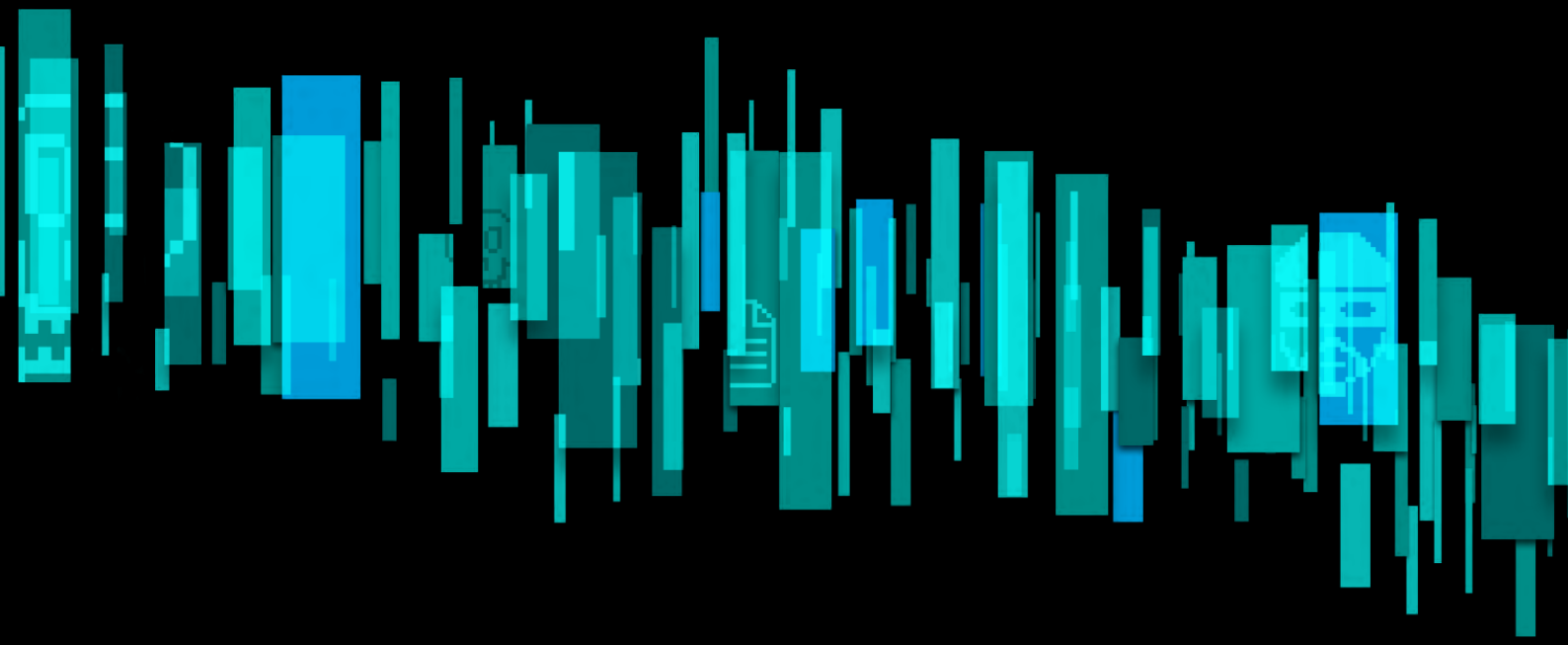
- Qui, au sein de mon entreprise, est ciblé par les attaques ?
- Quelles sont les failles actuelles dans les défenses ?
- Quelles sont mes priorités pour limiter les risques liés aux utilisateurs ?

Associez la threat intelligence à des formations de sensibilisation à la sécurité informatique à l'échelle de l'entreprise.

- Identifiez les utilisateurs les plus susceptibles d'être attaqués et ceux les plus susceptibles de se laisser piéger.
- Faites le lien entre le contenu de formation et les menaces en circulation.
- Apprenez à vos collaborateurs à identifier le phishing en vous appuyant sur de vrais leurres.

Instaurez une culture de la cybersécurité qui ne se limite pas aux formations.

- Les formations sont essentielles, mais elles ne suffisent pas.
- Une culture solide de la cybersécurité sur le lieu de travail encouragera les utilisateurs à prendre la sécurité des informations plus au sérieux dans leur vie personnelle.
- Évaluez les indicateurs pertinents et prenez des mesures de correction justes et appropriées.



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 75 % 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.

0400-013-03-01