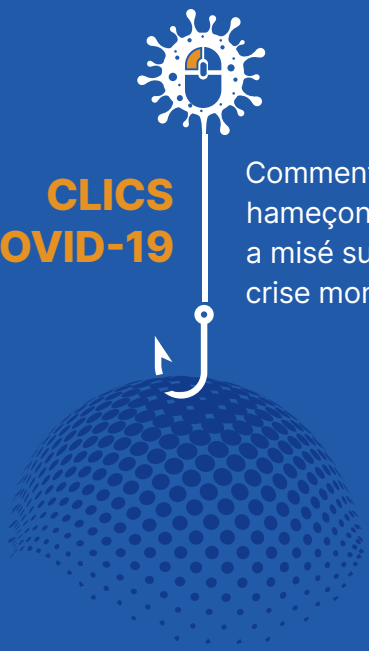
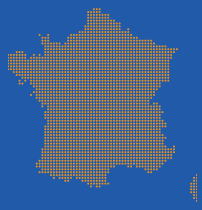


CLICS COVID-19

Comment le hameçonnage a misé sur une crise mondiale

POINTS IMPORTANTS À RETENIR

France



Le hameçonnage est une tactique cybercriminelle qui existe depuis longtemps. Alors, pourquoi une si vieille méthode de tromperie Internet est-elle encore si courante ? La réponse est simple : parce qu'elle est toujours très efficace.

Mais pourquoi les gens continuent-ils encore à cliquer ?

Nous avons interrogé 7 000 employés de bureau aux États-Unis, au Royaume-Uni, en Australie/Nouvelle-Zélande, en Allemagne, en France, en Italie et au Japon au sujet de leur compréhension du hameçonnage, de leurs habitudes de messagerie et de clic, et de la manière dont leur vie en ligne a changé depuis le début de la pandémie COVID-19. Nous avons ensuite travaillé avec le Dr Prashanth Rajivan, professeur adjoint à l'Université de Washington, pour comprendre pourquoi le hameçonnage fonctionne toujours.

Dans ce résumé analytique, nous mettons en évidence certaines statistiques les plus marquantes des répondants en France.

CARBONITE an opentext company | WEBROOT an opentext company

Dans l'ensemble, notre enquête suggère que les travailleurs français ne sont probablement pas bien préparés pour gérer les attaques de hameçonnage.

44 % seulement des personnes interrogées estiment en savoir suffisamment pour se protéger et protéger leurs données personnelles contre les cyberattaques.

8 sur 10 déclarent prendre des mesures pour déterminer si un e-mail peut être malveillant.

55 % admettent avoir cliqué sur un lien de hameçonnage l'année dernière.

Ce chiffre inquiétant est le pire score parmi tous les pays interrogés. La moyenne mondiale est de 3 sur 10. Parmi les répondants ayant été victimes de hameçonnage, 13 % ne l'ont jamais signalé.

Les habitudes de cyber-résilience des travailleurs français pourraient être meilleures.

64 % cliquent régulièrement sur des e-mails d'expéditeurs inconnus.

18 % d'entre eux le font « systématiquement », tandis que 46 % cliquent régulièrement sur les e-mails d'expéditeurs inconnus s'ils reconnaissent l'organisation que l'expéditeur prétend représenter ou si l'objet de l'e-mail correspond à leurs intérêts.

Environ 1 répondant sur 4 utilise ses appareils personnels à des fins professionnelles.

Le nombre de travailleurs français qui utilisent des appareils personnels à des fins professionnelles (26 %) est quasiment identique à la moyenne mondiale (25 %). Un pourcentage additionnel de 14 % des français interrogés utilisent leurs appareils professionnels à des fins personnelles et 39 % font les deux.

79 % ne sauvegardent pas leurs données.

Encore une fois, c'est le deuxième plus mauvais résultat. Malgré cela, 44 % affirment avoir dû récupérer des fichiers perdus depuis le début de la pandémie, ce qui est légèrement supérieur à la moyenne mondiale.

Seuls 8 % pensent que tous les employés devraient jouer un rôle dans la cyber-résilience de leur entreprise.

La moyenne mondiale est de 14 %, l'Australie/Nouvelle-Zélande atteint le pourcentage le plus élevé (27 %) et le Japon, le plus faible (7 %).

Impacts du COVID-19 et du travail à domicile

Plus de la moitié (58 %) a augmenté son temps de travail à domicile.

31 % sont plus préoccupés par le hameçonnage aujourd'hui qu'au début de l'année.

Plus de 1 répondant sur quatre (27 %) estime qu'il est mieux préparé à détecter le hameçonnage depuis qu'il travaille à domicile.

1 sur 5 (19 %) a reçu des e-mails de hameçonnage spécifiquement liés au COVID-19.

21 % déclarent que leur entreprise a renforcé les formations en cybersécurité pendant la pandémie.

Comment pouvons-nous tous nous améliorer ?

Consultez le rapport complet pour obtenir une image complète, découvrir comment ces chiffres s'harmonisent, lire l'analyse du Dr Rajivan et obtenir des conseils pratiques sur la façon dont les entreprises et les particuliers peuvent continuer à résister aux attaques de hameçonnage.

Visitez le site **https://mypage.webroot.com/covid-clicks-fr.html** pour télécharger votre exemplaire gratuit aujourd'hui.

À propos de Carbonite + Webroot

Les sociétés Carbonite, Webroot et OpenText exploitent le Cloud et l'intelligence artificielle pour fournir des solutions complètes de cyber-résilience aux entreprises, aux particuliers et aux fournisseurs de services gérés. La cyber-résilience signifie pouvoir rester opérationnel, même face aux cyberattaques et à la perte de données. C'est pourquoi nous avons uni nos forces pour fournir des solutions de protection des postes et des réseaux, de sensibilisation à la sécurité et de sauvegarde des données et de reprise après sinistre, ainsi que des services de renseignement sur les menaces utilisés par les principaux fournisseurs de technologies du marché dans le monde entier. Nous exploitons la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Webroot et Carbonite sont implantés en Amérique du Nord, en Europe, en Australie et en Asie. Découvrez la cyber résilience sur carbonite.com et webroot.com.