Phishing Insights 2021

Bien que le phishing existe depuis au moins un quart de siècle, il reste une technique de cyberattaque très efficace, parce qu'il continue d'évoluer chaque jour. Les attaquants sont prompts à identifier de nouvelles opportunités de phishing, dont la pandémie en a fourni de nombreuses, et à développer de nouvelles tactiques et techniques.

Pour les entreprises, le phishing marque souvent le point de départ d'une attaque complexe et multi-étapes. Les attaquants utilisent le phishing pour inciter les utilisateurs à installer des logiciels malveillants ou à partager leurs identifiants de connexion, permettant ainsi aux cybercriminels d'accéder à leur réseau. Un email en apparence inoffensif peut être l'élément déclencheur d'une attaque de ransomware, de cryptojacking ou d'un vol de données.

Ce présent rapport offre une vue actuelle du phishing basée sur une enquête indépendante menée auprès de 5 400 responsables informatiques qui y sont confrontés tous les jours dans le monde entier. Vous trouverez également une étude de cas d'une attaque de phishing réelle ayant conduit à un incident de ransomware coûtant plusieurs millions de dollars.

Selon le rapport « 2021 Data Breach Investigations » de Verizon, 36 % des vols de données confirmés impliquent des techniques de phishing (contre 25 % en 2019). Utilisez les résultats de cette enquête pour évaluer votre propre posture de sécurité en matière de phishing et pour identifier les moyens de renforcer vos défenses.

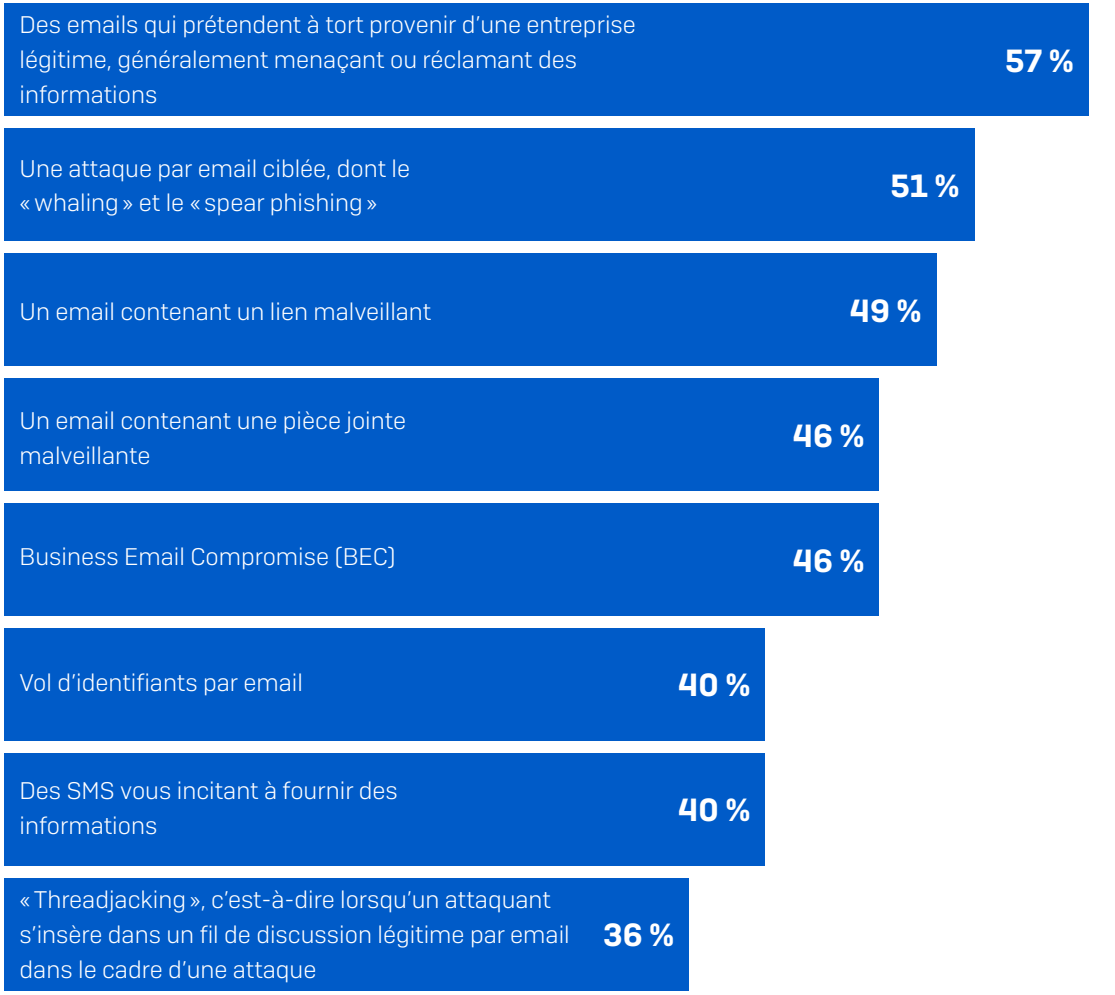
SOPHOS

1. Le phishing signifie différentes choses pour différentes personnes

Qu'est-ce que le phishing ? L'une des conclusions de notre enquête est que le phishing signifie différentes choses pour différentes personnes, même au sein des professionnels de l'informatique. La définition la plus couramment utilisée est : « *des emails qui prétendent à tort provenir d'une entreprise légitime, généralement menaçant ou réclamant des informations* ». Bien qu'il s'agisse de la réponse la plus populaire, moins de six personnes interrogées sur dix (57 %) ont choisi cette option, illustrant ainsi l'étendue des définitions possibles en matière de phishing.

46 % des répondants considèrent les attaques BEC (Business Email Compromise) comme étant du phishing et plus d'un tiers (36 %) considèrent le « threadjacking », c'est-à-dire lorsqu'un attaquant s'insère dans un fil de discussion légitime par email dans le cadre d'une attaque, comme du phishing.

Parmi les options ci-dessous, quelle est celle que vous considérez comme une attaque de phishing ?



Parmi ces options, quelle est celle que vous considérez comme une attaque de phishing ? [5 400] en excluant certaines options de réponse

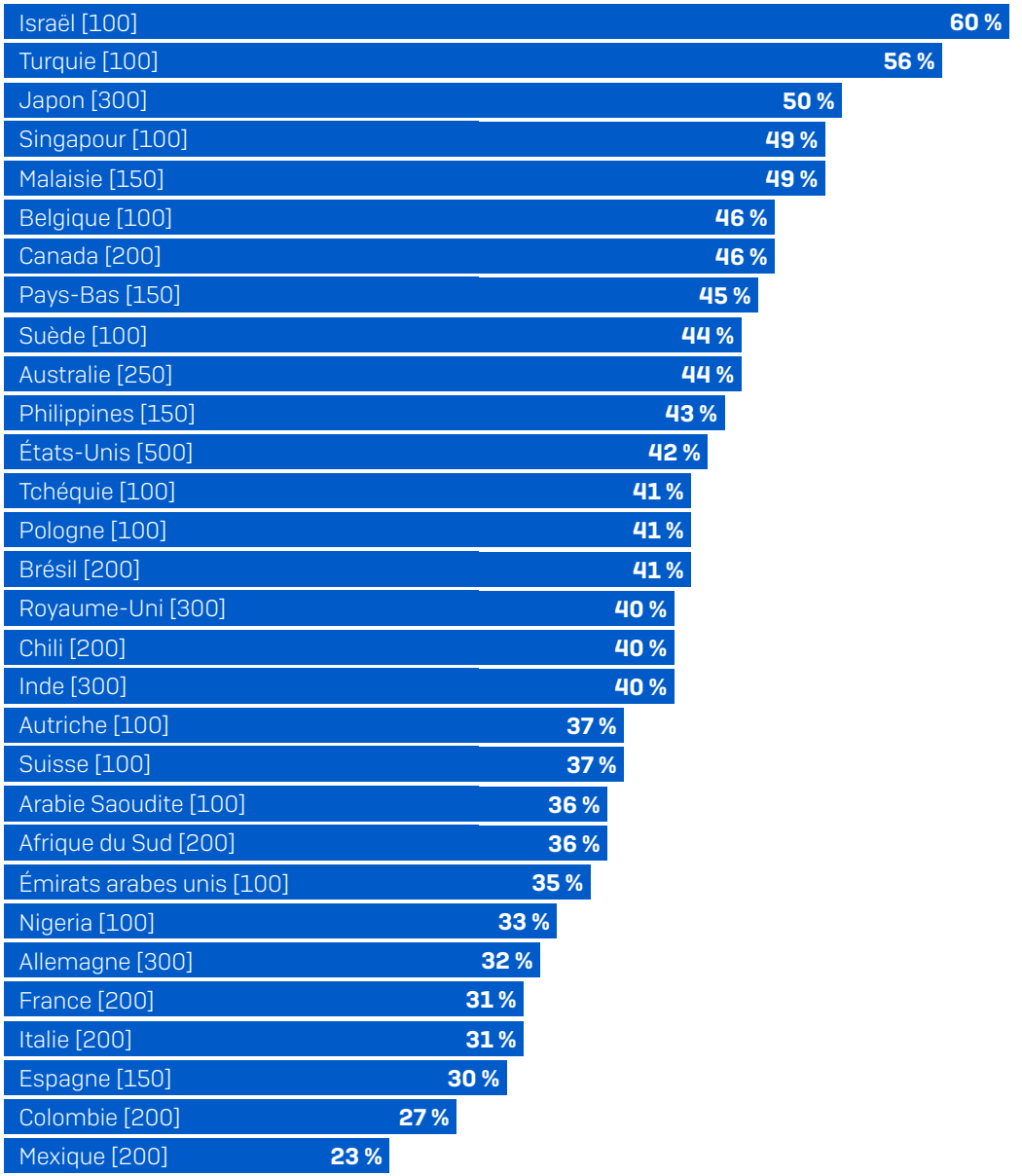
Les facteurs culturels ont un impact majeur sur la manière dont les utilisateurs perçoivent le phishing. Par exemple, la proportion de personnes interrogées qui considèrent que les SMS incitant à fournir des informations sont du phishing est plus de deux fois supérieure en Israël qu'au Mexique (60 % contre 23 %). Si de nombreux professionnels de l'informatique parlent dans ce cas de « smishing » plutôt que de phishing, les faux messages prétendant provenir de marques de confiance ont le même effet, indépendamment du mode de transmission.

Compte tenu des différences significatives dans la définition du phishing parmi les professionnels de l'informatique, il est raisonnable de s'attendre à un spectre similaire voire plus large d'interprétations parmi les employés non informaticiens.

Comprendre que la définition du terme « phishing » varie d'une personne à l'autre est important pour quiconque crée ou met en œuvre des programmes éducatifs visant à sensibiliser au phishing. Pour organiser des formations efficaces sur le phishing, il est important de trouver une définition commune du terme « phishing » afin de pouvoir replacer tout ce que nous apprenons dans son contexte.

POINT À RETENIR : LORSQUE VOUS FORMEZ VOS UTILISATEURS SUR LES RISQUES DU PHISHING, GARDEZ À L'ESPRIT QUE LE MOT « PHISHING » SIGNIFIE DIFFÉRENTES CHOSES POUR DIFFÉRENTES PERSONNES. SANS UN CONTEXTE CORRECT, LA FORMATION SERA MOINS EFFICACE.

Répondants considérant que les SMS vous incitant à fournir des informations sont du phishing.



Parmi ces options, quelle est celle que vous considérez comme une attaque de phishing ? [nombre total dans le graphique] Des SMS vous incitant à fournir des informations

2. Le phishing a considérablement augmenté depuis le début de la pandémie

70 % des personnes interrogées ont signalé une augmentation des attaques de phishing visant leur organisation depuis le début de la pandémie. Tous les secteurs ont été touchés, les administrations centrales connaissant la plus forte augmentation (77 %), suivi de près par les services aux entreprises et professionnels (76 %) et la santé (73 %).

La variation minime entre les secteurs (seulement 10 points de pourcentage avant l'arrondi*) montre que les cybercriminels attaquent sans discernement, en essayant de toucher le plus grand nombre de personnes possible pour augmenter leurs chances de réussite.

Les recherches des SophosLabs ont montré que les cybercriminels ont su exploiter rapidement les opportunités que leur offrait la pandémie et l'effacement des frontières entre le domicile et le travail. Voici quelques exemples :

- Augmentation rapide du télétravail. Les attaquants ont exploité le fait que les utilisateurs ont baissé leur garde le temps de s'habituer à leur nouvel environnement de travail à domicile.
- Augmentation des livraisons à domicile. Au cours des premiers mois de la pandémie, lorsque les personnes ont commencé à faire davantage d'achats en ligne, les emails de phishing se faisant passer pour des entreprises de transport de colis se sont multipliés.
- Inquiétude générale suscitée par la pandémie. Les cybercriminels ont exploité l'anxiété des gens et leur besoin d'information sur le Covid-19 en créant des arnaques sur le thème de la pandémie. Ils avaient anticipé le fait que le niveau élevé d'inquiétude pousserait les gens à ne pas vérifier la légitimité d'un message avant de cliquer.

Secteur	Répondants ayant connu une augmentation du nombre d'attaques de phishing contre leur organisation depuis le début de la pandémie.
Administrations centrales et AAI [117]	77 %
Services aux entreprises et professionnels [361]	76 %
Santé [328]	73 %
Médias, loisirs et divertissement [145]	72 %
Énergie, pétrole/gaz, services publics [197]	72 %
Commerce [435]	71 %
Éducation [499]	71 %
Autre [768]	71 %
Administrations locales [131]	69 %
Distribution et transport [203]	68 %
Services financiers [550]	68 %
Construction et immobilier [232]	68 %
Informatique, technologie et télécoms [996]	68 %
Manufacture et production [438]	66 %

Avez-vous constaté un changement dans le nombre d'attaques de phishing contre votre organisation depuis le début de la pandémie ? [nombre total dans le graphique] Oui, une forte augmentation ; Oui, une faible augmentation

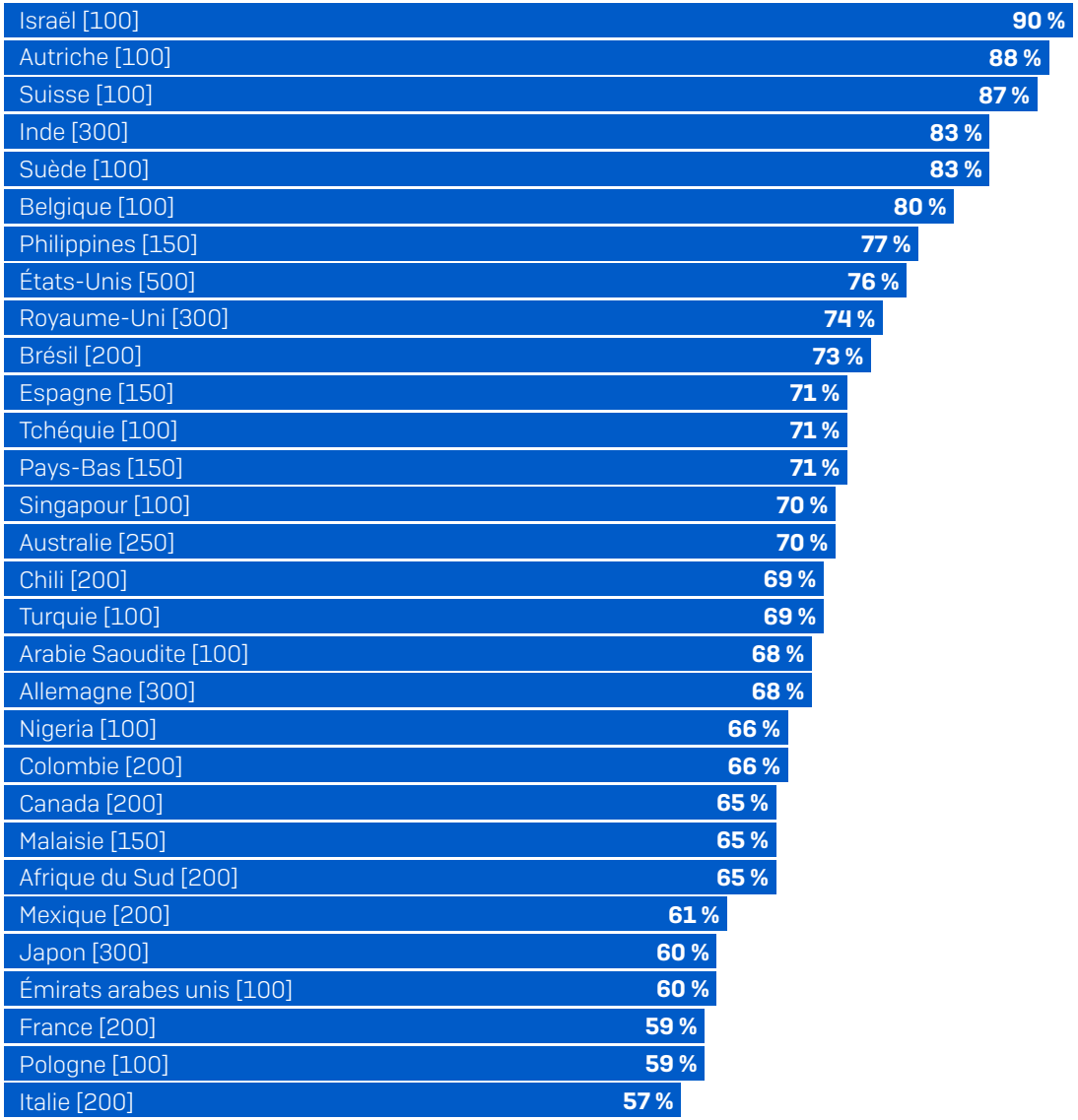
** Avant d'arrondir, 76,92 % des répondants de l'administration centrale ont signalé une augmentation, contre 66,43 % dans l'industrie manufacturière, ce qui donne un écart réel de 10,48 %.*

Si l'on constate peu de variations dans l'augmentation du nombre d'attaques de phishing entre les secteurs, l'enquête a révélé des différences considérables entre les pays depuis le début de la pandémie. Par exemple, 90 % des répondants en Israël ont signalé une augmentation du phishing, contre 57 % en Italie. Ces résultats, bien qu'influencés par la définition du terme « phishing » donnée par les répondants et par leur capacité à identifier et à mesurer les attaques, offrent un aperçu précieux de l'expérience réelle des équipes IT en première ligne.

La grande diversité des types d'emails de phishing s'explique par la grande diversité de cybercriminels qui se cachent derrière eux. Des groupes d'attaquants de haut vol concentrent généralement leurs attaques ciblées sur des pays dont le PIB est plus élevé, comme l'Autriche, la Suisse et la Suède, afin de maximiser leur rendement financier, ce qui contribue probablement à l'augmentation généralisée du phishing dans ces pays. Dans le même temps, le phishing est également utilisé dans le cadre d'attaques de masse de type « spray and pray », où un maximum de personnes est ciblé, dans l'espoir que quelqu'un finisse par se faire piéger.

POINT À RETENIR : NE RELÂCHEZ PAS VOS EFFORTS CONTRE LE PHISHING. LES CYBERCRIMINELS ONT DE PLUS EN PLUS RECOURS À CETTE TECHNIQUE ET AUCUN SECTEUR INDUSTRIEL NI AUCUN PAYS N'EST À L'ABRI.

Répondants ayant connu une augmentation du nombre d'attaques de phishing contre leur organisation depuis le début de la pandémie.



Avez-vous constaté un changement dans le nombre d'attaques de phishing contre votre organisation depuis le début de la pandémie ? [nombre total dans le graphique] Oui, une forte augmentation, Oui, une faible augmentation

3. La plupart des entreprises ont un programme de sensibilisation à la cybersécurité pour lutter contre le phishing

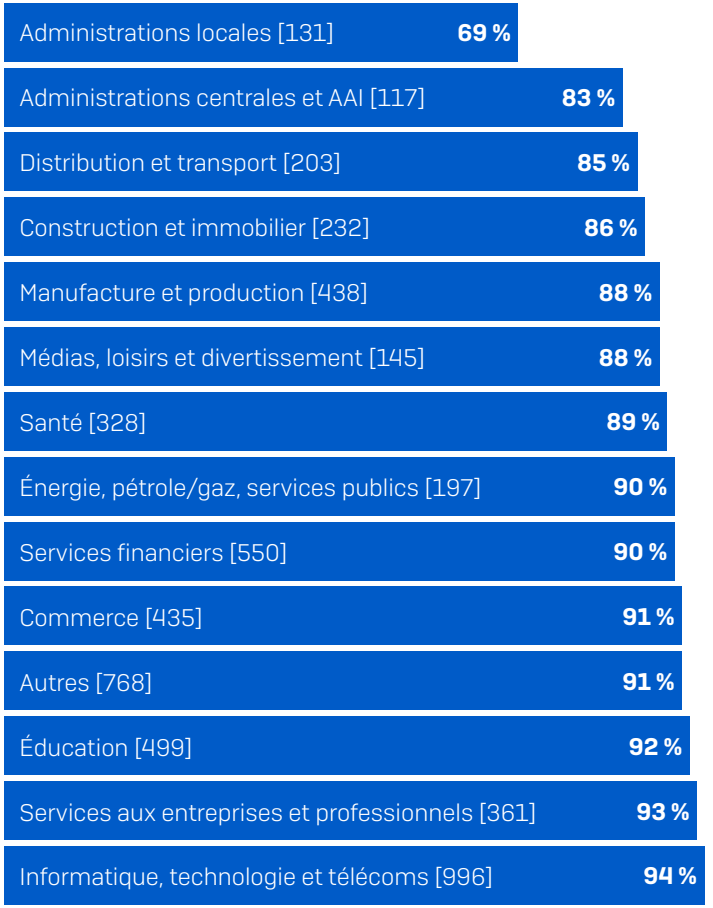
90 % des organisations ont mis en place un programme de sensibilisation au phishing, et 6 % prévoient d'en mettre un en place.

L'approche la plus populaire est la formation sur ordinateur, utilisée par 58 % des organisations. Plus de la moitié (53 %) ont recours à un formateur, et 43 % effectuent des simulations d'emails de phishing. 16 % des organisations combinent les trois techniques (formation sur ordinateur, formation animée par un formateur et simulations de phishing) dans leurs programmes de sensibilisation.

L'enquête a révélé que le secteur public est à la traîne lorsqu'il s'agit de mettre en place de tels programmes, les deux dernières places étant occupées par les administrations locales (69 %) et centrales (83 %). Cette situation est préoccupante, car les organismes gouvernementaux sont les cibles fréquentes de cyberattaques à fort impact : les administrations centrales sont les plus susceptibles de subir des attaques par ransomware de type extorsion, tandis que les administrations locales sont les plus susceptibles de voir leurs données chiffrées lors d'une attaque par ransomware.

POINT À RETENIR : SI VOUS FAITES PARTIE DES 10 % QUI N'ONT PAS ENCORE DE PROGRAMME DE SENSIBILISATION AU PHISHING, METTEZ-EN UN EN PLACE SANS TARDER.

Utilisation de programmes de sensibilisation au phishing



Votre organisation a-t-elle mis en place un programme de sensibilisation à la cybersécurité pour lutter contre le phishing ? [5400] Oui, nous organisons des programmes de formation sur ordinateur ; Oui, nous organisons des programmes de formation animés par un formateur ; Oui, nous organisons des simulations de phishing.

90%

ont implémenté un programme de sensibilisation au phishing

58%

organisent un programme de formation sur ordinateur

53%

organisent un programme de formation animé par un formateur

43%

organisent des simulations d'emails de phishing

Votre organisation a-t-elle mis en place un programme de sensibilisation à la cybersécurité pour lutter contre le phishing ? [5400] Oui, nous organisons des programmes de formation sur ordinateur ; Oui, nous organisons des programmes de formation animés par un formateur ; Oui, nous organisons des simulations de phishing.

4. Les programmes de sensibilisation au phishing sont bien établis

Près des deux tiers (65 %) des programmes de sensibilisation au phishing ont été mis en œuvre il y a 1 à 3 ans, ce qui reflète la réponse des organisations au changement de technique des attaquants dans les années 2010. L'amélioration des cyberdéfenses contre les attaques sur le Web au milieu des années 2010 a forcé les attaquants à se tourner vers de nouveaux vecteurs tels que les emails. Cela a, en retour, créé un fort besoin de programmes d'éducation des utilisateurs.

Compte tenu de l'augmentation généralisée du phishing depuis le début de la pandémie, il est encourageant de constater que 98 % des organisations avaient mis en place leur programme de sensibilisation au phishing avant l'arrivée du Covid-19. Grâce à ces programmes, les employés auront été bien formés pour résister au déluge d'emails de phishing reçus en 2020.

Quand votre organisation a-t-elle mis en place le programme de sensibilisation au phishing ?	
L'année dernière	2 %
Il y a 1 ou 2 ans	30 %
Il y a 2 ou 3 ans	35 %
Il y a 3 ou 4 ans	20 %
Il y a 4 ou 5 ans	12 %
Il y a plus de 5 ans	0 %
Ne sait pas	1 %

Répondants dont l'organisation a mis en place un programme de sensibilisation au phishing [4866].

POINT À RETENIR : VEILLEZ À REVOIR ET À METTRE À JOUR RÉGULIÈREMENT VOS SUPPORTS ET VOS ACTIVITÉS DE SENSIBILISATION AU PHISHING POUR VOUS ASSURER QU'ILS SONT TOUJOURS PERTINENTS ET INTÉRESSANTS POUR VOS UTILISATEURS.

5. Le suivi des actions positives est essentiel pour évaluer l'efficacité d'une formation

Presque toutes les organisations (98 %) dotées d'un programme de sensibilisation des utilisateurs au phishing évaluent l'impact de leurs efforts. La mesure et le suivi des résultats permettent aux organisations d'optimiser leurs programmes pour en retour améliorer les résultats.

Les approches les plus courantes consistent à suivre le nombre d'emails de phishing signalés au service informatique (68 %) ou le niveau de signalement du phishing par les utilisateurs (65 %). Il est encourageant de constater que ces mesures positives, qui reflètent une bonne sensibilisation et un bon comportement des utilisateurs, sont les plus répandues. Identifier un email de phishing et le signaler permet aux équipes IT d'empêcher les autres utilisateurs de se faire piéger.

La moitié des organisations (50 %) effectuent un suivi du taux de clics dans les emails de phishing. Bien qu'il s'agisse d'une mesure négative (elle met l'accent sur le fait de tomber dans le piège), le taux de clics fournit aux équipes IT des données qui les aident à cibler les programmes de sensibilisation là où ils sont le plus nécessaires et à adapter le contenu aux réalités de leur organisation. Plus vous pouvez suivre de points de données, tant positifs que négatifs, mieux c'est.

POINT À RETENIR : REVOYEZ RÉGULIÈREMENT VOS PROGRAMMES D'ÉDUCATION DES UTILISATEURS À LA LUMIÈRE DES RÉSULTATS DE VOS ÉVALUATIONS ET CONCENTREZ-VOUS SUR LA RECONNAISSANCE ET LA CÉLÉBRATION DES COMPORTEMENTS POSITIFS.

98%
évaluent l'impact de leur programme de sensibilisation

68%
effectuent un suivi du nombre de tickets liés au phishing signalé au service informatique

65%
effectuent un suivi du niveau de signalement des emails de phishing par les utilisateurs

50%
effectuent un suivi du taux de clics dans les emails de phishing

Que suivez-vous pour évaluer l'impact de votre programme de sensibilisation ? [4 866 répondants dont l'organisation a mis en place un programme de sensibilisation au phishing]. Nombre de tickets liés au phishing signalés au service informatique ; Niveau de signalement des emails de phishing par les utilisateurs ; Taux de clics dans les emails de phishing. Nous n'évaluons pas l'impact de nos programmes de sensibilisation au phishing. Exclue certaines options de réponse

Étude de cas : du phishing à une attaque de ransomware à plusieurs millions de dollars

L'équipe Sophos Rapid Response a récemment été appelée pour aider une entreprise confrontée à une attaque de ransomware majeure. Une fois l'attaque maitrisée, l'équipe Rapid Response a investigué l'incident pour comprendre son origine. Voici ce qu'elle a découvert :

Trois mois avant l'attaque, un employé a reçu un email de phishing qui semblait venir d'un collègue d'un autre bureau. Il est probable que les attaquants aient accédé au compte de messagerie du collègue pour piéger d'autres employés et leur faire croire que l'email était légitime.

Le message était très court et écrit dans un mauvais anglais. Il demandait à l'employé de cliquer sur un lien pour vérifier un document. Le lien était en fait un lien malveillant et lorsque l'employé l'a cliqué, les attaquants ont obtenu les identifiants d'accès de l'administrateur de domaine.

L'équipe Rapid Response pense que cet email de phishing a été envoyé par un Initial Access Broker (IAB), un cybercriminel dont le travail consiste à obtenir un accès à l'environnement de l'entreprise victime, puis de le vendre à d'autres criminels qui vont l'exploiter dans leur attaque (ransomware, vol de données, etc.).

Ici, l'équipe informatique de la victime est intervenue et a mis fin à l'attaque de phishing. La situation semblait être réglée.

Pourtant, huit semaines plus tard, un acteur malveillant a installé et exécuté deux outils : Cobalt Strike et PowerSploit PowerView, sur l'ordinateur de la victime. Il s'agit d'outils commerciaux utilisés en toute légitimité par les pen-testeurs, mais aussi par les cybercriminels à des fins malveillantes. Les attaquants ont probablement utilisé PowerView pour effectuer une reconnaissance du réseau et Cobalt Strike pour assurer ensuite la persistance sur ce réseau.

Plus aucune activité n'est ensuite identifiée au cours des deux semaines suivantes. L'équipe Rapid Response pense que cette période correspond au moment où l'Initial Access Broker s'est mis en quête d'un acheteur pour les identifiants d'accès.

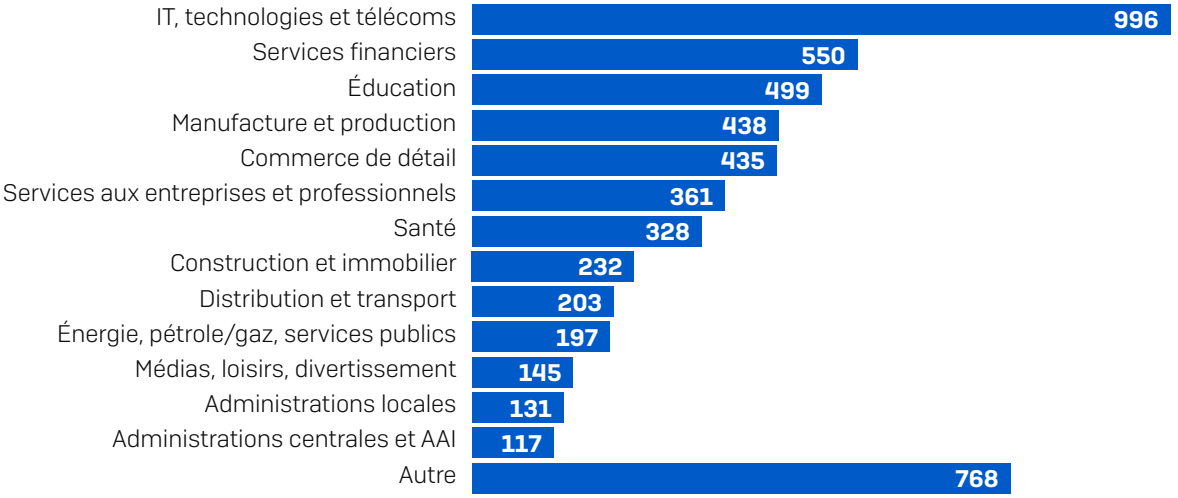
Une fois ces derniers vendus, les nouveaux « propriétaires » en ont très rapidement tiré profit. Ils sont apparus sur le réseau, ont installé Cobalt Strike sur d'autres machines et ont commencé à collecter et à voler des données.

Trois mois après l'email de phishing initial, les attaquants ont lancé le ransomware Revil à 4 h du matin, heure locale, et réclamé une rançon de 2,5 millions de dollars.

À propos de l'enquête

Sophos a demandé à l'institut de recherche indépendant Vanson Bourne d'interroger 5400 décideurs informatiques dans des entreprises de taille moyenne (100 à 5000 employés) dans 30 pays. Cette enquête s'est déroulée entre janvier et février 2021. Les répondants provenaient à la fois de secteurs privés que de secteurs publics/gouvernementaux.

Nombre de répondants par secteur



Nombre de participants par pays

Pays	Nb de répondants	Pays	Nb de répondants	Pays	Nb de répondants
Allemagne	300	EAU	100	Nigeria	100
Afrique du Sud	200	Espagne	150	Pays-Bas	150
Arabie Saoudite	100	États-Unis	500	Philippines	150
Australie	250	France	200	Pologne	100
Autriche	100	Inde	300	République tchèque	100
Belgique	100	Israël	100	Royaume-Uni	300
Brésil	200	Italie	200	Singapour	150
Canada	200	Japon	300	Suède	100
Chili	200	Malaisie	150	Suisse	100
Colombie	200	Mexique	200	Turquie	100

2021-08-13 WPFR (NP)

SOPHOS