proofpoint.

Le rapport State of the Phish en bref

INTRODUCTION

En temps normal, la cybersécurité peut s'avérer délicate. Dans des périodes tumultueuses, telles que la pandémie mondiale qui bouleverse profondément nos environnements de travail, elle peut devenir extrêmement compliquée. L'année dernière, les professionnels de la sécurité des informations ont été confrontés à une explosion des escroqueries de phishing sur le thème du coronavirus et à la progression continue des attaques de ransomwares, tout en devant assurer la protection des utilisateurs pendant leur migration brutale vers le télétravail.

Notre rapport *State of the Phish* 2021 examine ces tendances et aborde bien d'autres sujets. Il analyse les données recueillies dans le cadre d'enquêtes, de simulations d'attaques de phishing et de cyberattaques réelles pour vous offrir un éclairage sur les menaces actuelles les plus dévastatrices et les principales vulnérabilités des utilisateurs. Il fait également le point sur les mesures à prendre pour vous en prémunir.

Voici un aperçu des principales conclusions du rapport.

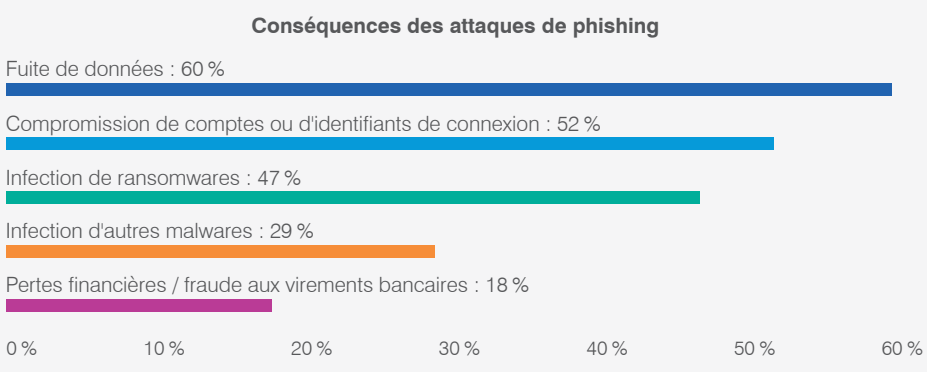
LES MENACES PRENNENT DE L'AMPLEUR

2020 a été une année exceptionnelle pour les attaques de phishing, qui ont fait de nombreuses victimes par le biais de diverses techniques.

57 %

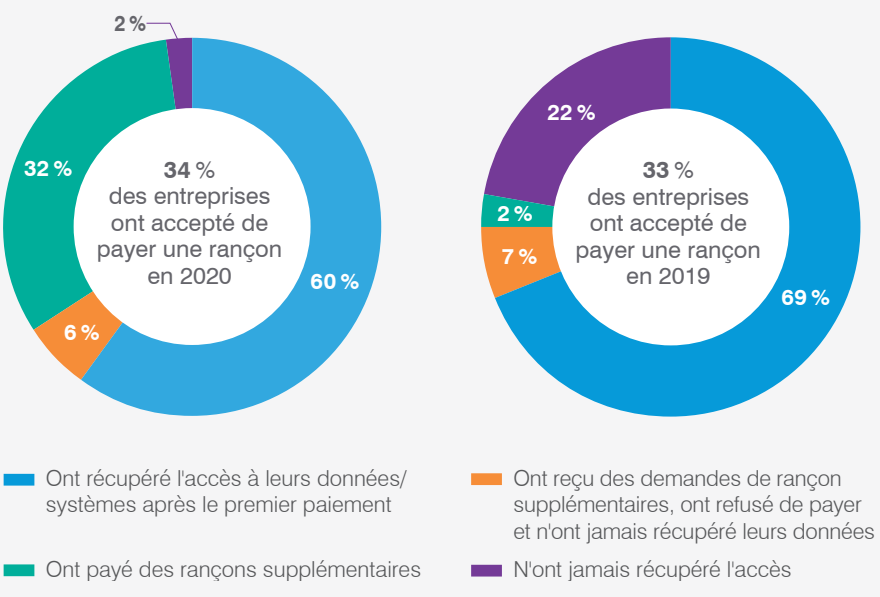
des professionnels interrogés dans le cadre d'une enquête indépendante ont déclaré que leur entreprise a été victime d'une attaque de phishing fructueuse en 2020, contre **55 %** en 2019.

Conséquences des attaques de phishing



Un pourcentage légèrement plus élevé de victimes de ransomwares ont payé la rançon en vue de récupérer l'accès à leurs données et à leurs systèmes. Elles sont toutefois moins nombreuses à avoir obtenu ce qui leur avait été promis, et près d'un tiers ont finalement payé une rançon supplémentaire.

Résultats suite au paiement de rançons (2020 et 2019)



INTERNATIONAL

68 % des entreprises américaines ont admis avoir payé une rançon en 2020, soit deux fois plus que la moyenne mondiale.

41 % des entreprises espagnoles ont refusé de payer une rançon suite à une infection, ce qui fait d'elles les moins enclines à négocier avec les cybercriminels.

78 % des entreprises françaises ont eu la chance de récupérer l'accès à leurs données et à leurs systèmes après avoir payé une seule rançon, soit le pourcentage le plus élevé parmi les pays sondés (les États-Unis occupent la deuxième place avec **76 %**).

14 % des entreprises allemandes ont refusé de payer une rançon supplémentaire, soit le pourcentage le plus élevé parmi les pays sondés.

PRINCIPALES VULNÉRABILITÉS DES UTILISATEURS

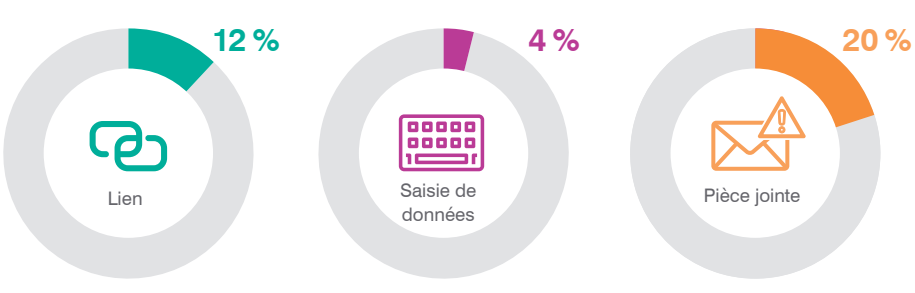
Les attaques d'aujourd'hui ciblent les personnes, pas seulement les technologies. Il est essentiel d'identifier les principales vulnérabilités des utilisateurs pour renforcer leur résilience.

Plus d'un utilisateur sur dix a cliqué sur un email de simulation d'attaque de phishing, tandis qu'un sur cinq s'est laissé piéger par un email de simulation d'attaque de phishing contenant une pièce jointe.

Taux d'échec moyen des tests de phishing

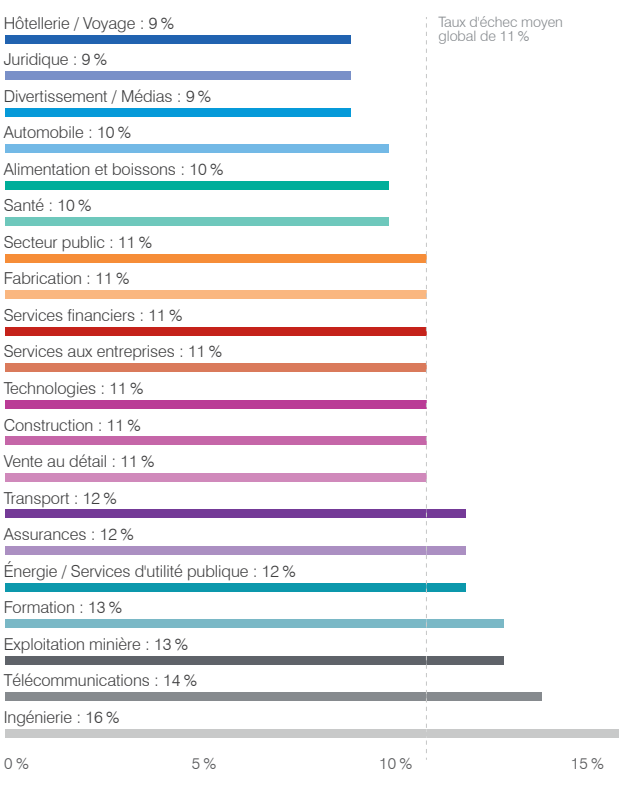
11 %

Types de modèles de phishing : taux d'échec moyen

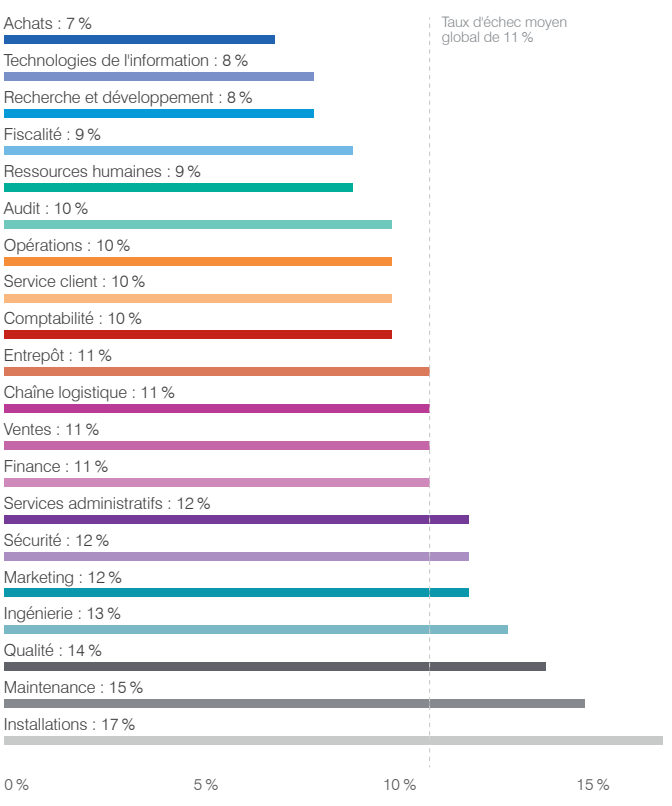


Les utilisateurs de certains secteurs sont plus vulnérables que d'autres. Il en va de même pour les départements.

Taux d'échec moyen par secteur d'activité



Taux d'échec moyen par département



Les termes de cybersécurité courants peuvent paraître évidents pour les responsables informatiques, mais de nombreux utilisateurs ne les comprennent pas.

Notre questionnaire à choix multiple sur la définition de certains termes de cybersécurité comportait trois réponses et une option « Je ne sais pas ». Les utilisateurs qui ne connaissent pas la réponse à une question peuvent présenter autant de risques que ceux qui donnent une mauvaise réponse.

	Bonnes réponses	Mauvaises réponses	Je ne sais pas
Qu'est-ce que le **PHISHING ?**	63 %	22 %	15 %
Qu'est-ce qu'un **RANSOMWARE ?**	33 %	36 %	31 %
Qu'est-ce qu'un **MALWARE ?**	65 %	21 %	14 %

Les collaborateurs américains ont obtenu les moins bons résultats (52 % de bonnes réponses).

Les collaborateurs britanniques ont obtenu les meilleurs résultats (69 % de bonnes réponses).

Seuls 26 % des collaborateurs allemands ont répondu correctement.

42 % des collaborateurs australiens ont répondu correctement.

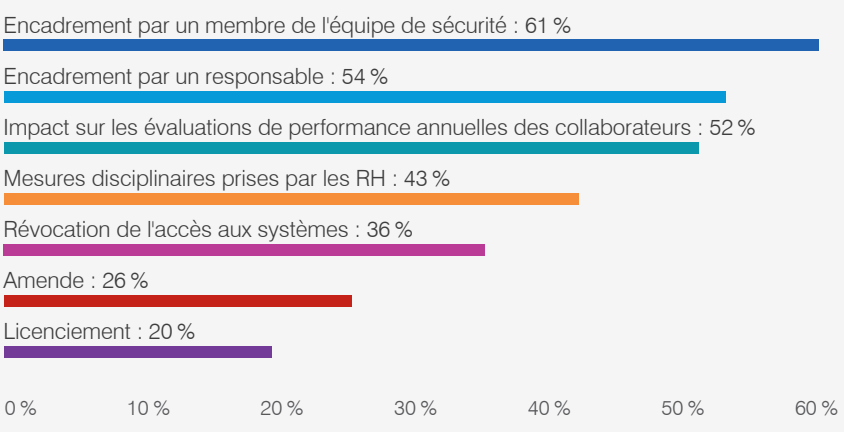
Les collaborateurs espagnols ont obtenu les meilleurs résultats (75 % de bonnes réponses).

Les collaborateurs américains ont obtenu des résultats en dessous de la moyenne (54 % de bonnes réponses).

MESURES PRISES PAR LES ENTREPRISES

Bien que nous ne recommandions pas de sanctionner les utilisateurs pour les erreurs qu'ils commettent de bonne foi, certaines entreprises utilisent une modélisation des conséquences pour les « récidivistes ».

Conséquences pour les récidivistes



INTERNATIONAL

82 % des entreprises américaines ont mis en place une modélisation des conséquences, soit le pourcentage le plus élevé parmi les pays sondés.

72 % des entreprises australiennes demandent aux RH de prendre des mesures disciplinaires contre les récidivistes.

35 % des entreprises espagnoles ont mis en place une modélisation des conséquences, soit le pourcentage le plus faible parmi les pays sondés.

32 % des entreprises britanniques ont affirmé que leur modélisation des conséquences n'a eu aucun impact sur la sensibilisation des collaborateurs.

30 % des entreprises américaines ont recours au licenciement comme conséquence, soit le pourcentage le plus élevé parmi les pays sondés.

TÉLÉCHARGEZ LE RAPPORT COMPLET

Vous souhaitez en savoir plus ? Le rapport *State of the Phish* 2021 inclut des données issues des échantillons suivants :

Une enquête indépendante menée auprès de **3 500** adultes actifs de sept pays (Allemagne, Australie, Espagne, États-Unis, France, Japon et Royaume-Uni)	Une enquête indépendante menée auprès de **600** professionnels de la sécurité informatique de ces mêmes pays	Plus de **60 millions** de simulations d'attaques de phishing envoyées par nos clients sur une période de 12 mois	Environ **15 millions** d'emails signalés par les utilisateurs de nos clients

Téléchargez le rapport pour obtenir un aperçu détaillé des menaces de phishing actuelles et des mesures que vous pouvez prendre pour mettre en place une stratégie de cybersécurité centrée sur les personnes permettant de réduire les risques et de renforcer la sensibilisation et la résilience des utilisateurs.

www.proofpoint.com/fr/resources/threat-reports/state-of-phish

proofpoint.