proofpoint.

RÉSUMÉ

State of the Phish 2020

La messagerie électronique est le moyen de communication d'entreprise le plus critique, mais aussi le principal vecteur de menaces.

C'est par ce biais que les cybercriminels sont le plus susceptibles de toucher leurs cibles : vos collaborateurs. À l'aide d'une multitude de techniques de phishing diversifiées, ils incitent vos utilisateurs à cliquer sur des liens dangereux, à révéler leurs identifiants ou même à se plier directement à des demandes (par exemple, en transférant des fonds ou en envoyant des fichiers sensibles).

Pour mieux comprendre cette menace, notre sixième rapport annuel *State of the Phish* présente les conclusions d'enquêtes réalisées auprès de professionnels de la sécurité des systèmes d'information et d'utilisateurs finaux. Le rapport analyse également plus de 50 millions d'emails de simulation d'attaques de phishing envoyés par nos clients à leurs utilisateurs sur une période de 12 mois. Dans ce contexte, nous évaluons leur connaissance de la terminologie et des pratiques de cybersécurité. Nous analysons par ailleurs les menaces de phishing auxquelles les équipes de sécurité des systèmes d'information sont confrontées. Enfin, nous expliquons comment les entreprises peuvent adopter une approche centrée sur les personnes de la gestion des menaces de phishing actuelles.

Voici nos principales observations :

Sensibilisation des utilisateurs : enquête mondiale auprès de 3 500 employés d'entreprise

- Seulement 61 % ont correctement identifié la définition du phishing dans un questionnaire à choix multiple.
- Seulement 31 % ont correctement identifié la définition du ransomware.
- La génération Y continue à être moins performante que les autres tranches d'âge (y compris les baby boomers) en ce qui concerne la reconnaissance des termes clés.
- De nombreux sondés n'appliquent pas les bonnes pratiques de base en matière de cybersécurité :
  - 45 % admettent réutiliser leurs mots de passe.
  - Plus de 50 % ne protègent pas leur réseau Wi-Fi domestique par un mot de passe.
  - 32 % ignorent ce qu'est un VPN, ou réseau privé virtuel.
- 90 % des employés utilisent leurs appareils d'entreprise pour des activités d'ordre privé. Près de 50 % laissent des amis ou des membres de leur famille utiliser leurs appareils d'entreprise.

Problèmes informatiques : enquête mondiale auprès de 600 professionnels de la sécurité des systèmes d'information

- 55 % des entreprises ont subi au moins une attaque de phishing en 2019.
- La plupart des entreprises ont subi des tentatives d'ingénierie sociale employant diverses méthodes :
  - Spear phishing (harponnage) : 88 %
  - Piratage de la messagerie en entreprise (BEC, Business Email Compromise) : 86 %
  - Réseaux sociaux : 86 %
  - SMiShing (phishing par SMS/texte) : 84 %
  - Vishing (phishing vocal) : 83 %
  - Attaques par clé USB : 81 %
- 33 % des entreprises internationales ont été infectées par un ransomware en 2019 et ont choisi de payer la rançon. (32 % supplémentaires ont été infectés mais ont refusé de payer.) Parmi les entreprises qui ont négocié avec les maîtres-chanteurs :
  - 9 % ont reçu des demandes de rançon supplémentaires.
  - 22 % n'ont jamais récupéré l'accès à leurs données, même après avoir payé la rançon.
- 85 % des entreprises ne proposent pas à leurs utilisateurs un bouton pour le signalement des emails suspects, ce qui complique la tâche des équipes de sécurité qui souhaitent faire participer les utilisateurs à la lutte contre le phishing.
- 78 % des entreprises affirment avoir observé une diminution de leur vulnérabilité au phishing grâce aux formations de sensibilisation à la sécurité.

Actions des utilisateurs : analyse des données Proofpoint

- Les utilisateurs finaux des clients Proofpoint ont signalé près de 9,2 millions d'emails suspects en 2019, soit 67 % de plus qu'en 2018. Rien qu'au troisième trimestre 2019, les utilisateurs ont informé leurs équipes de sécurité de la présence de milliers de menaces sérieuses :
  - Près de 20 000 attaques de phishing axées sur les identifiants de connexion
  - Plus de 4 000 attaques dont la charge virale contenait des malwares, notamment des chevaux de Troie d'accès à distance, des portes dérobées (backdoor) et des voleurs d'informations à haut risque
- Les taux de signalement plus élevés indiquent que les utilisateurs sont plus attentifs aux leurres de phishing. Ces utilisateurs sont plus susceptibles d'avertir les équipes de sécurité de la présence de messages suspects de manière générale, ce qui améliore les défenses globales contre le phishing. De ce fait, lors de l'analyse des résultats des tests de simulations d'attaques de phishing, mieux vaut se focaliser sur les taux de signalement plutôt que sur les taux d'échec pour évaluer le niveau de réussite. Par exemple :
  - Les utilisateurs finaux des secteurs de l'enseignement et des services financiers ont enregistré le même taux d'échec moyen lors des simulations d'attaques de phishing : 8 %.
  - Par comparaison, les entreprises du secteur financier présentaient le taux de signalement le plus élevé (20 %) lors des tests de phishing, tandis que les établissements d'enseignement enregistraient le taux le plus bas (5 %).
- Les cibles et les méthodes des cybercriminels peuvent varier de façon significative au fil du temps, et les VAP (Very Attacked People™ ou personnes très attaquées) ne sont pas toujours les personnes aux postes les plus importants.
- Les entreprises doivent adopter une approche de leurs vulnérabilités davantage axée sur les personnes et responsabiliser leurs collaborateurs pour qu'ils deviennent une ligne de défense plus robuste. Elles doivent avoir conscience que n'importe quel utilisateur peut devenir une cible à tout moment, et utiliser leurs données et leurs informations de cyberveille pour mettre au point un programme de sensibilisation à la sécurité qui couvre à la fois l'entreprise dans son ensemble et des types d'utilisateurs ciblés.

Principales observations : États-Unis

- Seulement 49 % des collaborateurs aux États-Unis ont correctement identifié la définition du phishing.
- Les collaborateurs américains sont les moins méfiants à l'égard des réseaux Wi-Fi publics : 45 % pensent que les emplacements de confiance (comme les bars ou les hôtels) offrent toujours des réseaux sécurisés.
- Plus de 70 % des collaborateurs américains permettent à leurs amis et aux membres de leur famille d'utiliser leurs appareils d'entreprise.

Principales observations : EMEA

- Les collaborateurs allemands ont été les plus nombreux à identifier correctement la définition du phishing (66 %).
- Les collaborateurs français ont été les plus nombreux à reconnaître les définitions du SMiShing (54 %) et du vishing (48 %).
- Les collaborateurs espagnols ont enregistré le taux de reconnaissance le plus élevé pour la définition de malware (79 %), mais le plus faible pour celle du ransomware (22 %).
- Les collaborateurs au Royaume-Uni étaient les moins bien informés en ce qui concerne les protections Wi-Fi : 21 % ont affirmé qu'ils ne sécurisaient pas leur réseau domestique parce qu'ils ne savaient pas comment procéder.
- Les entreprises du Royaume-Uni sont les plus susceptibles d'imposer une sanction financière aux collaborateurs qui ont été victimes à plusieurs reprises d'attaques de phishing (21 %). Les entreprises françaises sont les plus enclines à licencier ces « récidivistes » (13 %).
- Toutes les entreprises espagnoles ont subi des tentatives d'ingénierie sociale et de SMiShing en 2019.
- Plus de la moitié des entreprises allemandes qui ont choisi de payer la rançon après une attaque de ransomwares n'ont jamais récupéré l'accès à leurs données.

Principales observations : APAC

- Les collaborateurs australiens ont été les plus nombreux à correctement identifier la définition du ransomware (42 %).
- Les collaborateurs australiens sont les plus susceptibles d'affirmer qu'ils n'ont pas besoin de VPN sur leurs appareils (34 %).
- Environ 60 % des entreprises australiennes seulement ont affirmé avoir subi des attaques d'ingénierie sociale, de SMiShing et de vishing en 2019, bien en deçà des moyennes mondiales.
- Plus de 20 % des collaborateurs japonais affirment réutiliser un ou deux mots de passe pour tous leurs comptes en ligne.
- Les collaborateurs japonais sont ceux qui ont été les moins nombreux à identifier la définition du SMiShing (17 %).
- Seulement 42 % des entreprises japonaises ont subi une attaque de phishing fructueuse en 2019 (un chiffre bien inférieur à la moyenne mondiale de 55 %).
- Seulement 10 % des entreprises japonaises ont payé la rançon demandée à la suite d'une attaque de ransomware en 2019.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.