

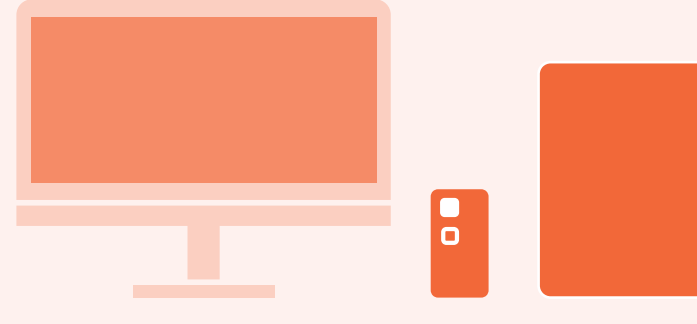
Tendances critiques en matière de phishing mobile

Principales conclusions de notre rapport annuel sur l'état du phishing Global State of Mobile Phishing Report

Le phishing mobile est l'un des moyens les plus courants utilisés par les attaquants pour voler les identifiants de connexion des employés. Le travail à distance et la popularité du BYOD (bring your own devices) ont considérablement augmenté la fréquence de ces attaques. Par conséquent, le nombre d'employés victimes de phishing augmente à un rythme alarmant.

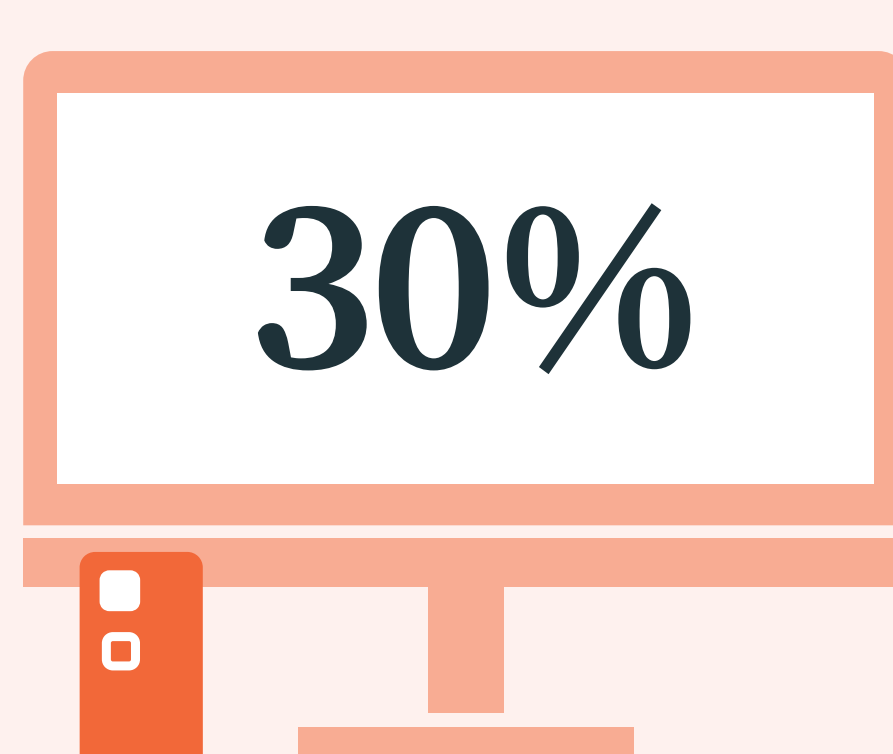
[Lire le rapport](#)

L'assouplissement des politiques de BYOD a créé des angles morts pour les équipes de sécurité et informatiques.



En 2022, **plus de 50%** des appareils personnels ont été exposés à des attaques de phishing.

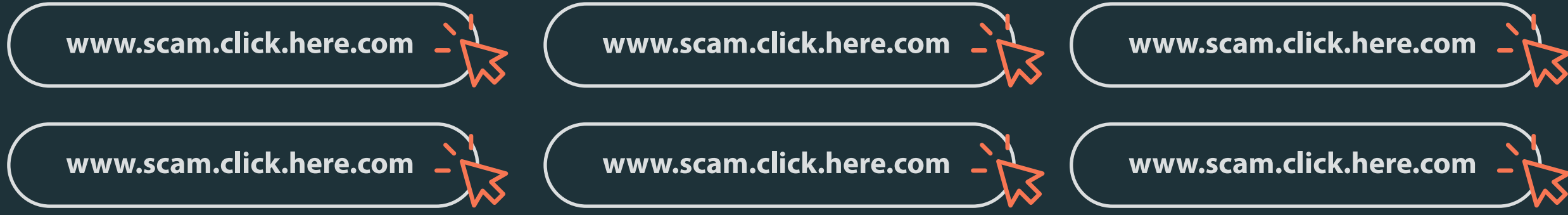
et **plus de 30%** des appareils mobiles personnels et d'entreprise ont été la cible d'attaques de phishing au moins quatre fois.



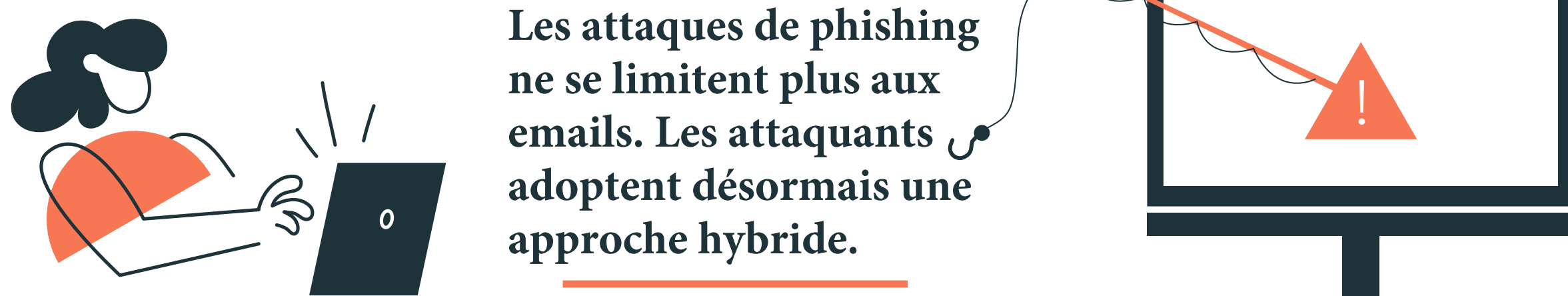
Les attaques de phishing sont plus difficiles à détecter.



Plus de 40% d'entre eux ont cliqué sur au moins six liens malveillants.



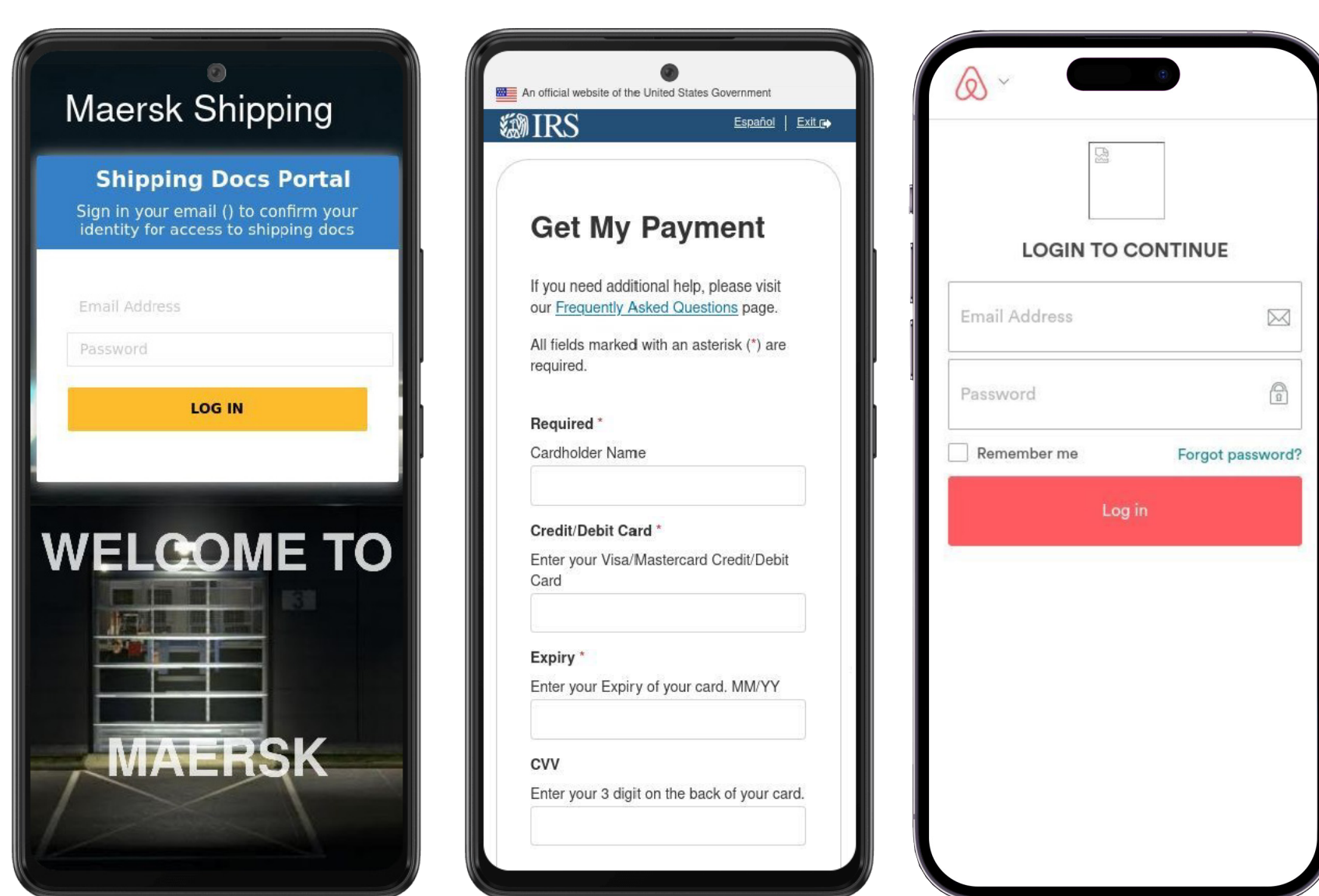
Les tactiques de phishing ne se limitent plus aux emails.



Les attaques de phishing ne se limitent plus aux emails. Les attaquants adoptent désormais une approche hybride.

Les attaquants utilisent une combinaison de vishing (phishing vocal), smishing (phishing par SMS) et quishing (phishing par QR code) pour compromettre directement les informations d'identification d'un employé ou contourner d'autres mesures de sécurité telles que l'authentification multifactorielle (MFA).

Les attaques de phishing hybrides ont été **multipliées par plus de 7** au deuxième trimestre 2022 en comparaison avec le premier trimestre 2021.

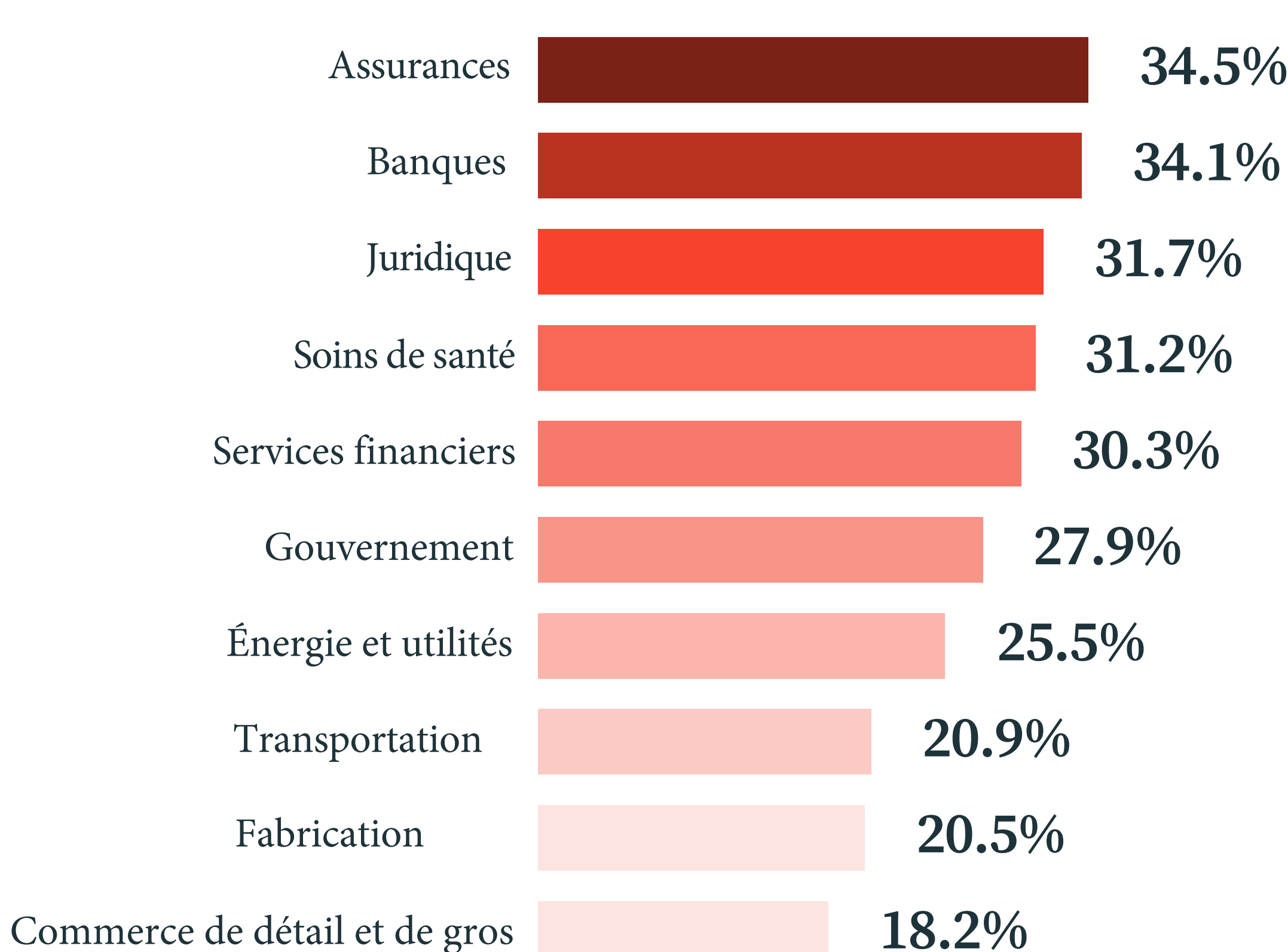


Impact financier d'une attaque de phishing mobile

\$ **3 8 7 6 5 5 0**

Votre secteur d'activité présente-t-il un risques élevé ?

Certaines des industries les plus réglementées sont régulièrement la cible de phishing. Cela est probablement dû à la quantité importante d'informations et de données sensibles qu'elles détiennent (par exemple, PII, PHI, propriété intellectuelle ou données financières).



Pour plus d'informations sur les taux de détection de phishing dans votre région, consultez notre [cartographie mondiale interactive](#).

Pour en savoir plus sur l'état mondial du phishing mobile, [téléchargez notre rapport annuel](#).