

QUI PEUT ÊTRE CIBLÉ ?

Les cadres, les équipes de vente et le conseil d'administration

Quels sont les postes les plus ciblés par les attaques de phishing ?

Les cadres, les membres du conseil d'administration et les équipes de vente sont les plus exposés aux tentatives de phishing. Ce n'est pas surprenant : ces personnes bénéficient d'un accès, d'une influence et d'une image publique. La bonne nouvelle, c'est que leurs taux de clics sont souvent inférieurs à ceux des autres employés.

Événements de phishing parmi les rôles hautement ciblés

80+ Les dirigeants reçoivent plus de 80 attaques de phishing par utilisateur et par an

60 Les membres du conseil d'administration reçoivent 60 attaques de phishing par utilisateur et par an

75 Les équipes de vente reçoivent 75 attaques de phishing par utilisateur et par an

Les mesures que les professionnels de la sécurité peuvent prendre

La cybersécurité commence et se termine avec les personnes. Pour maintenir un faible taux de clics dans ce groupe très ciblé, suivez ces étapes :

ÉTAPE 1

Tirer parti d'une formation et d'une intervention spécifiques aux risques : utilisez l'analyse comportementale avancée pour dispenser une formation ciblée aux employés qui occupent des postes plus exposés aux attaques de phishing.

ÉTAPE 2

Améliorer la visibilité des risques : veillez à ce que l'analyse des risques basée sur l'utilisateur ne se limite pas aux exercices de simulation de phishing.

ÉTAPE 3

Développer des protections basées sur les rôles : déployez des couches supplémentaires de protection et de surveillance pour ces personnes. Il s'agit notamment de réduire leur exposition dans les situations où elles sont en contact avec le public.

ÉTAPE 4

Adopter un cadre holistique de gestion des risques humains : intégrez les technologies de sécurité à une stratégie centrée sur l'humain qui favorise l'engagement et la responsabilité continus.

Approfondissez ce sujet en lisant l'intégralité du [rapport Exposer le risque humain ici](#).