Smishing and Executive Impersonation Protection

Proactively mitigate mobile risks

Mobile devices are cornerstones of enterprise productivity, communication, and identity verification. Most importantly, they frequently act as the second form of authentication for multi-factor authentication (MFA) solutions. Leaving iOS and Android devices vulnerable to phishing and social engineering attacks exposes the soft underbelly of any organization.

Key Challenges

Evolving tactics: As the traditional cyber kill chain evolves and threat actors take on modern tactics, SMS-based phishing and executive impersonation are two of the most effective ways to trick employees into sharing corporate login credentials and sensitive information.

How Lookout helps: With Smishing and Executive Impersonation Protection, Lookout provides a critical new layer of protection against the modern kill chain with robust, proactive protections against social engineering and executive impersonation attacks.

Lack of visibility: IT and security teams lack visibility into this significant threat and the ability to block it, which leaves their organization at high risk of compromise.

How Lookout helps: In-depth reporting helps admins understand when a coordinated attack is targeting their organization. Lookout enables security teams to implement proper precautions and communicate out to their employees before someone falls victim.

Incomplete protection: Most solutions only cover a piece of what Lookout can provide on the device and lack reporting capabilities in their administrator console. This leaves a massive operational and security gap in that organization's security posture.

How Lookout helps: Smishing and Executive Impersonation Protection work equally across iOS and Android, can redirect suspicious messages from the end user and grant industry-first visibility into these threats with admin reporting capabilities.

Why Lookout

IT and Security admins can now gain previously unseen insights into when a coordinated attack is targeting their organization and ensure protections are in place with frictionless deployment on employee devices.

Lookout addresses unique pain points with smishing and executive impersonation by providing comprehensive protection against these sophisticated social engineering tactics. Lookout's solution detects inbound messages with malicious intent by analyzing specific parameters like unknown numbers and high-pressure language patterns, all while maintaining user privacy. This helps identify and mitigate threats before they can exploit human vulnerabilities within your organization.

To see how it works, watch this interactive demo: demo.lookout.com/psl/h0208z2

© 2024 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.