Lookout

SURVEY REPORT

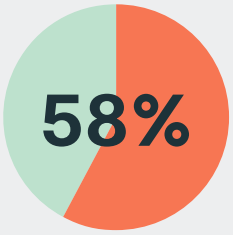
The Mobile Security Mirage:
Unmasking Dangerous Misconceptions

A recent global survey by Lookout of over 700 security leaders revealed a concerning disconnect between belief and reality when it comes to cybersecurity preparedness. The belief is that employees are prepared for the highly effective modern tactics that threat actors use such as mobile-focused social engineering, executive impersonation, and phishing. The reality, proven by the results of this survey, tells a different story and masks a dangerous situation that leaves businesses overconfident and more vulnerable to modern threats than they realize.

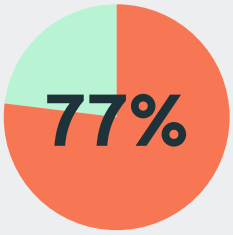
The survey's top findings highlight pervasive overconfidence in employees to be able to identify modern threats. For instance, 96% of leaders are confident their employees can spot a phishing attempt that comes via their mobile devices. Yet, more than half reported incidents where employees fell victim to executive impersonation scams via text message or voice, leading to financial loss or sensitive data exposure.

Furthermore, despite more than 75% of organizations experiencing at least one mobile phishing attack in the last six months, only half of respondents are very concerned. What's more is that over half of social engineering incidents go unnoticed or unreported, which creates a massive security blind spot. Even with widespread security training efforts, "lack of training" remains the top reason cited for employees clicking suspicious links, suggesting that current education may not be keeping pace with the rapid evolution of sophisticated threats.

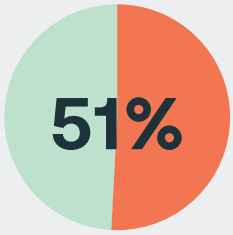
The most critical insights:



of companies have experienced incidents due to executive impersonation scams via text or voice.



of respondents have experienced one or more attacks in the past six months.

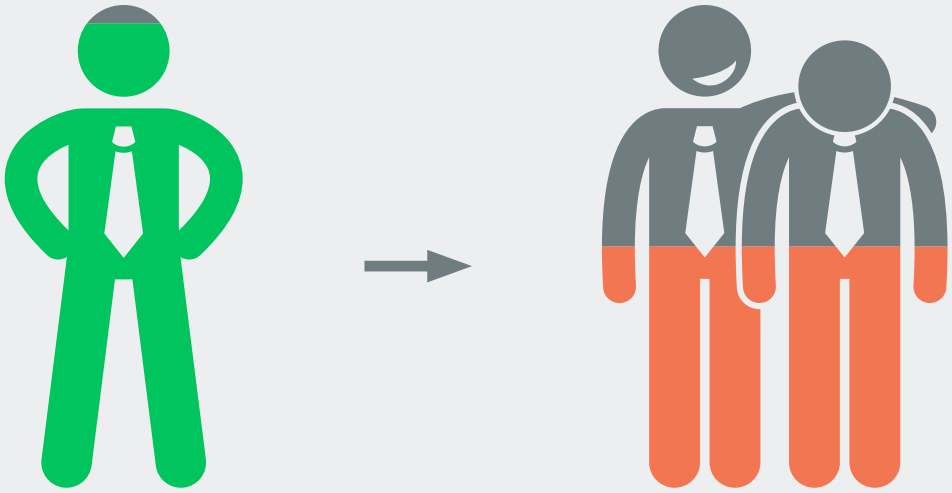


admit to having inconsistent visibility of social engineering attempts.

The Hidden Hurdles: Why Cyber Defenses Fall Short

These findings highlight core issues for organizations. For one, there's a dangerous gap between how ready organizations feel they are for security threats and how prepared they actually are. This overconfidence can lead to successful attacks, even when teams think they're protected. Today's threat actors want to quietly access enterprise data, and the best way to do that is with an employee's username and password. Since these actors know that mobile endpoints have historically been an afterthought of endpoint security strategies, they aggressively target employees on their iOS and Android devices to compromise their credentials.

One of the most effective tactics when targeting employees on mobile is social engineering, which is incredibly effective when delivered via SMS, voice, messaging apps, or any other mobile form factor. Since traditional security solutions cannot grant visibility into these attacks, Most of these manipulative attempts simply go unnoticed until it's too late, making it incredibly tough to defend against them. Similarly, security training doesn't seem to be able to keep up with modern tactics either. Whether the issue is that training isn't engaging enough, happening often enough, or evolving fast enough, it seems unable to truly prepare employees for today's evolving threats.



96%

of leaders are confident their employees can spot a phishing attempt...

yet, more than half reported incidents where employees fell victim to executive impersonation scams via text message

Actionable Strategies for a Safer Future

The data shows that employees and their mobile devices are squarely in the sights of threat actors – representing the first step in the modern cyber kill chain that eventually leads to data compromise. To address these pressing challenges, organizations must adopt a multi-faceted approach that can secure their front line.

To handle the baseline of mobile-focused threats, security teams can implement a mobile threat defense (MTD) solution to protect employees against social engineering, phishing, malware, device, and network attacks. MTD solutions should take an AI-first approach to combat the constantly evolving threats that bombard mobile users and devices.

They should then gain the required visibility into more strategic mobile security datapoints, such as vulnerable assets and web traffic analysis, by integrating mobile endpoint detection and response (EDR) into their existing SIEM, SOAR, EDR, or XDR solutions. These two steps will grant organizations the visibility, detection, and actionability required to protect against modern threats that aim to exploit human behavior.

Finally, organizations should supplement modern solutions with sophisticated and ongoing security awareness training specifically designed for mobile-centric threats, including simulated phishing and social engineering exercises that reflect current malicious tactics. This training should foster a culture of vigilance and easy, judgment-free reporting.

The findings in this survey underscore a critical need for organizations to reassess their cybersecurity strategies, moving beyond mere confidence to implement robust solutions that provide real-time visibility and proactive protection against the ever-changing threat landscape.

To learn more about how Lookout is helping secure thousands of organizations and their employees against mobile-centric threats, visit www.lookout.com.

*The data presented in this report is sourced from the independent research company Censuswide, which conducted the survey in June 2025.

Lookout

About Lookout

Lookout, Inc. is a **globally recognized cybersecurity leader** delivering advanced protection for the **most vulnerable element** of any enterprise security strategy — human error and manipulation. **Cloud-native by design**, the Lookout platform offers rapid, scalable deployment and simplified security operations, **defending the frontline** of **human-centric attacks**—the mobile device.

Attackers now target the **human element** more than ever, with mobile devices providing the **most direct path to their victims**. Using **social engineering techniques** that exploit basic human instincts like trust, curiosity, and urgency, they deceive users into revealing sensitive credentials, allowing them to slip past legacy security solutions.

Lookout Endpoint Detection and Response (EDR) continuously monitors mobile endpoints for signs of **human-centric attacks**, as well as traditional malware, software vulnerabilities, and other anomalous activity. It uses advanced threat detection techniques, including **artificial intelligence (AI)** and behavioral analysis, to identify threats before they escalate across the enterprise.

Learn more at www.lookout.com and follow us on the Lookout Blog, LinkedIn, and X.

Request a demo at
www.lookout.com/request-a-demo