


Concerning Trends in Mobile Phishing Attacks

Lookout survey reveals critical gaps in mobile security that could compromise cloud data

Participants: **250** U.S.-based CISOs and cybersecurity leaders

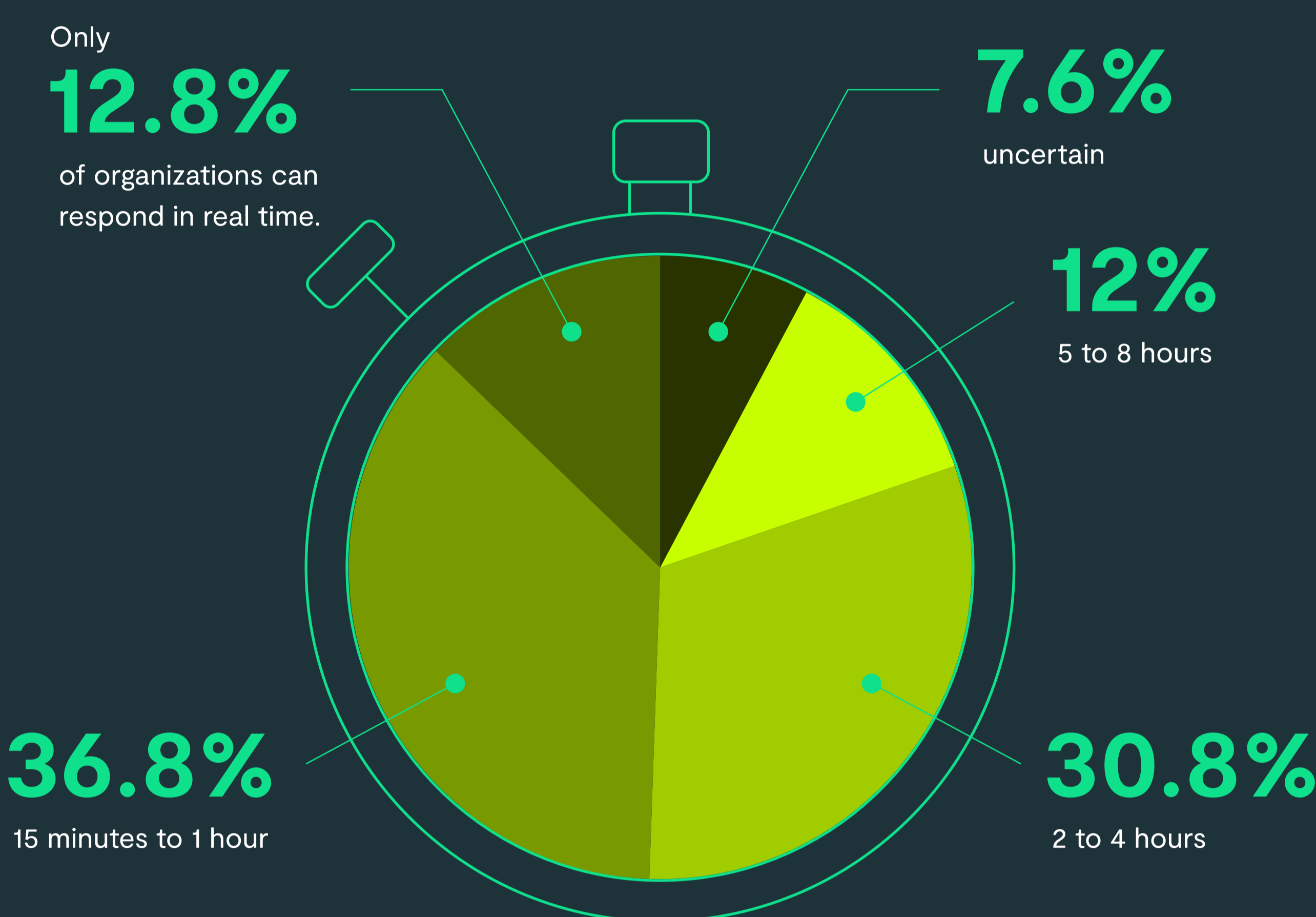
Key Findings

THREAT PERCEPTION	
<p>97%</p> <p>believe malicious mobile applications or permissions pose a threat.</p>	<p>75%</p> <p>experienced mobile phishing attempts in the last six months.</p>
ATTACK EXAMPLES	
	<p>Scattered Spider Attacks:</p> <ul style="list-style-type: none"> Accounts compromised within minutes Internal social engineering on Slack, email, Microsoft Teams Data stolen within five minutes

The Modern Kill Chain, as defined by Lookout, emphasizes that it is crucial to respond to an attack immediately.

Ability to Respond Quickly Cause for Concern

SURVEY RESULTS ON RESPONSE TIMES




DELAYS DUE TO
<ul style="list-style-type: none"> Insufficient automation Overwhelming data volume

Internal Defense Exercise

Results showed that **less than one-third** of respondents conduct internal simulations of various phishing scenarios, including SMS phishing, social engineering, QR code phishing or voice phishing.

Threat Landscape

SOCIAL ENGINEERING TACTICS	
<ul style="list-style-type: none"> Target mobile phones for credentials Example: Attackers posing as IT team members 	
COST OF A DATA BREACH	
<p>\$4.45 million</p> <p>(Global average in 2023, 15% increase over three years)</p> <p><small>Source: IBM Cost of a Data Breach Report 2023</small></p>	

The Lookout Defense-in-Depth Approach

- Protects against the modern kill chain
- Largest database of threat telemetry
- Lookout Cloud Security Platform: Swiftly stops modern breaches

[Read the full report](#) →

The data is sourced from the independent research company Censuswide which, in April 2024, surveyed 250 U.S.-based CISOs and other mobile and cloud cybersecurity leaders.