Lookout SMS Phishing Awareness Tool

Elevate security awareness with real-time mobile phishing simulations

Mobile phishing is the primary entry point for cyber attacks

Mobile phishing has become increasingly common and difficult for businesses to identify and protect against. It only takes one link tap for a user to unknowingly initiate a cyber attack or data breach.

Phishing attacks targeting mobile users have high success rates because of how difficult it is to spot the tell-tale signs of a malicious message compared to receiving them on a laptop or desktop. Smaller screens, the speed at which we operate with mobile devices, and our inherent trust in these devices greatly increases the likelihood of a successful attack.

44%

Over two-fifths (44%) of those that had suffered a mobile related security breach said that user behavior was a contributing factor.[1]

On mobile a vast majority of phishing attacks (85%) happen outside of email — including through SMS, social media, and even gaming apps.[2] SMS-based phishing, or smishing, has become one of the most common tactics used by attackers to deliver deceptive messages and convince the target to take actions that may compromise themselves or their device. Smishing campaigns rely on social engineering to exploit human trust and trick the recipient into clicking on a malicious link.

How vulnerable are your users to mobile phishing attacks?

Find out!

The Lookout SMS Phishing Awareness Tool can be used by organizations to understand how susceptible employees are to clicking on mobile phishing links. As mobile continues to be central to your employees' workflow, this is a great way to understand and educate on the risk these devices pose to your organization.

How does the SMS phishing awareness tool work?

Lookout will help your organization prepare a mock phishing campaign through the following steps:

1. Create a short SMS message that is relevant to your business and employees.
2. Customize the sender name to simulate a socially-engineered campaign.
3. Create a landing page that the link in the message leads to. This will include a custom message and your company logo.
4. Once the required content and timing is agreed, Lookout will push the SMS campaign to your employees.
5. Once the phishing message has been sent to your employees, you will receive a report broken down by individual employees and mobile operating systems.

[1,2] 2022 Verizon Mobile Security Index Report

How does this benefit you?

Historically, anti-phishing training and tools were focused on desktop computers and email messages. But with hybrid work becoming the norm, it's critical that organizations understand and mitigate the risk from mobile phishing attacks.

What do we need to get started?

- A CSV file with the following format: username;phone number (we do not require actual user names)
- A signed **Lookout MPRA Agreement** — this will be a direct engagement with Lookout and your organization

What data do we collect?

- User's phone number, which are stored anonymously in our system database (4 first digits and 2 last)
- We identify and capture information about who has clicked on the phishing link
- Once the results have been passed across to the customer, the campaign is deleted from the system

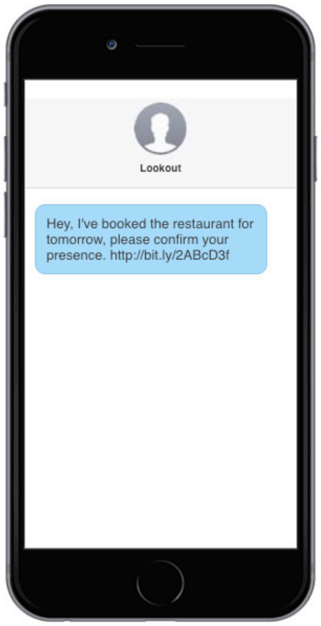
About Lookout Phishing and Content Protection

Lookout Phishing and Content Protection is included with Lookout Mobile Endpoint Security to to monitor and secure secure against phishing threats. It works to detect phishing attacks from any mobile channel, across any network, in a privacy-aware manner.

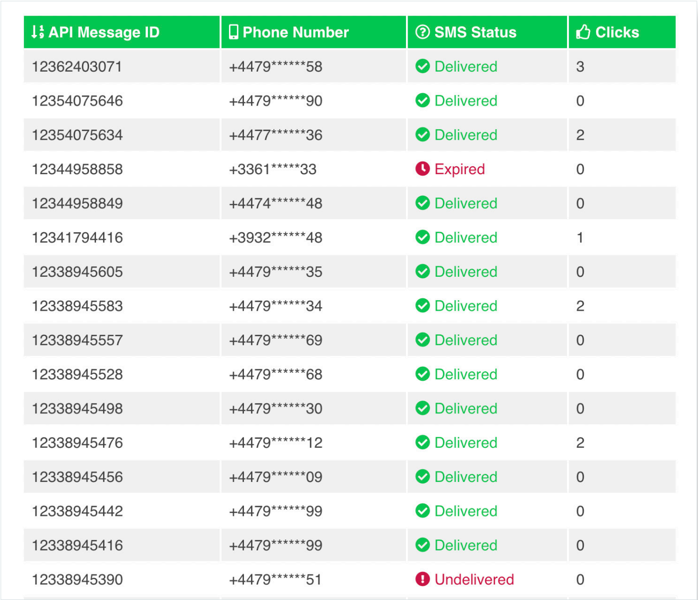
By analysing all web requests made by the mobile device and apps without inspecting the content itself, Lookout protects against mobile phishing without violating end user privacy. Instead, web requests such as URLs are compared with malicious URLs identified within the Lookout Security Graph. If a phishing site is identified, the URL is blocked and alerts are sent to both end users and administrators.

Lookout Phishing and Content Protection also allows your organization to apply web filtering controls to prevent users from visiting harmful, denylisted, or offensive web content from mobile devices.

Contact your Lookout partner to arrange your mobile phishing awareness campaign.



Hey, I've booked the restaurant for tomorrow, please confirm your presence. http://bit.ly/2ABcD3f



API Message ID	Phone Number	SMS Status	Clicks
12362403071	+4479******58	✓ Delivered	3
12354075646	+4479******90	✓ Delivered	0
12354075634	+4477******36	✓ Delivered	2
12344958858	+3361*****33	Expired	0
12344958849	+4474******48	✓ Delivered	0
12341794416	+3932******48	✓ Delivered	1
12338945605	+4479******35	✓ Delivered	0
12338945583	+4479******34	✓ Delivered	2
12338945557	+4479******69	✓ Delivered	0
12338945528	+4479******68	✓ Delivered	0
12338945498	+4479******30	✓ Delivered	0
12338945476	+4479******12	✓ Delivered	2
12338945456	+4479******09	✓ Delivered	0
12338945442	+4479******99	✓ Delivered	0
12338945416	+4479******99	✓ Delivered	0
12338945390	+4479******51	! Undelivered	0

Lookout™

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

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