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 errant link tap for a user to unknowingly kick off 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 an attack that people recognise on a laptop or desktop. Smaller screens, the speed at which we operate with mobile devices, and our inherent trust in these devices can greatly increase the likelihood of a successful attack.

44%

Over two-fifths (44%) of those that had suffered a mobile related security breach said that user behaviour 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 perhaps the most common tactic used by attackers to deliver deceptive messages and convince the target to 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 organisations to understand how susceptible employees are to clicking links on mobile that they believe have genuinely been sent by their employer. This is a great way to measure risk and integrate that knowledge into your broader security strategy.

How does the SMS phishing awareness tool work?

Lookout will help your organisation prepare a harmless socially engineered phishing campaign by working with you through the following steps:

1. Create a short SMS message that sounds relevant to your business and employees.
2. Customise 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. As your employees receive the message, the resulting statistics will be provided and broken down by individual employees and mobile operating systems.

[1,2] 2022 Verizon Mobile Security Index Report

How does this benefit you?

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

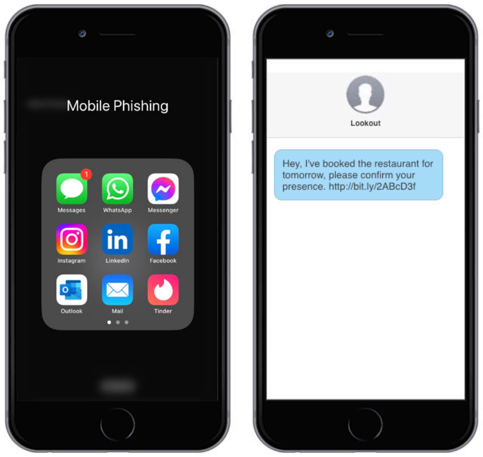
Phishing attacks targeting mobile users have high success rates because of how difficult it is to spot the tell-tale signs of an attack that people recognise on a laptop or desktop. Smaller screens, the speed at which we operate with mobile devices, and our inherent trust in these devices can greatly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

What do we need to get started?

- A CSV file with the following format: User1;+44771233245, (we do not require user names)
- A signed **Lookout MPRA Agreement –** this will be a direct engagement with Lookout and each organisation

What data do we collect?

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



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

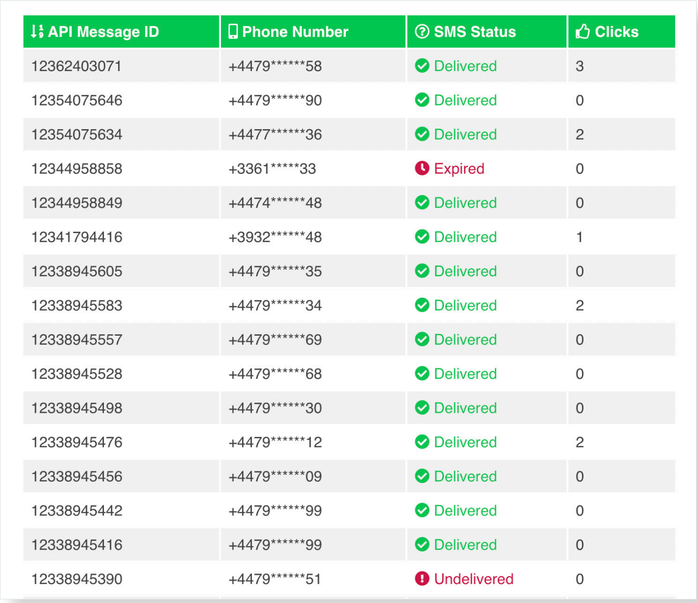
About Lookout Phishing and Content Protection

Lookout Phishing and Content Protection is included within Lookout Mobile Endpoint Security to effectively 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 is able to protect against mobile phishing while protecting end user privacy. Web requests (e.g., URLs) are compared with malicious URLs identified within the Lookout Security Graph. Access to phishing sites are blocked and alerts are sent to both end users and admins.

Lookout Phishing and Content Protection also allows your organisation 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.



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

© 2022 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20221019-Lookout-USv1.0