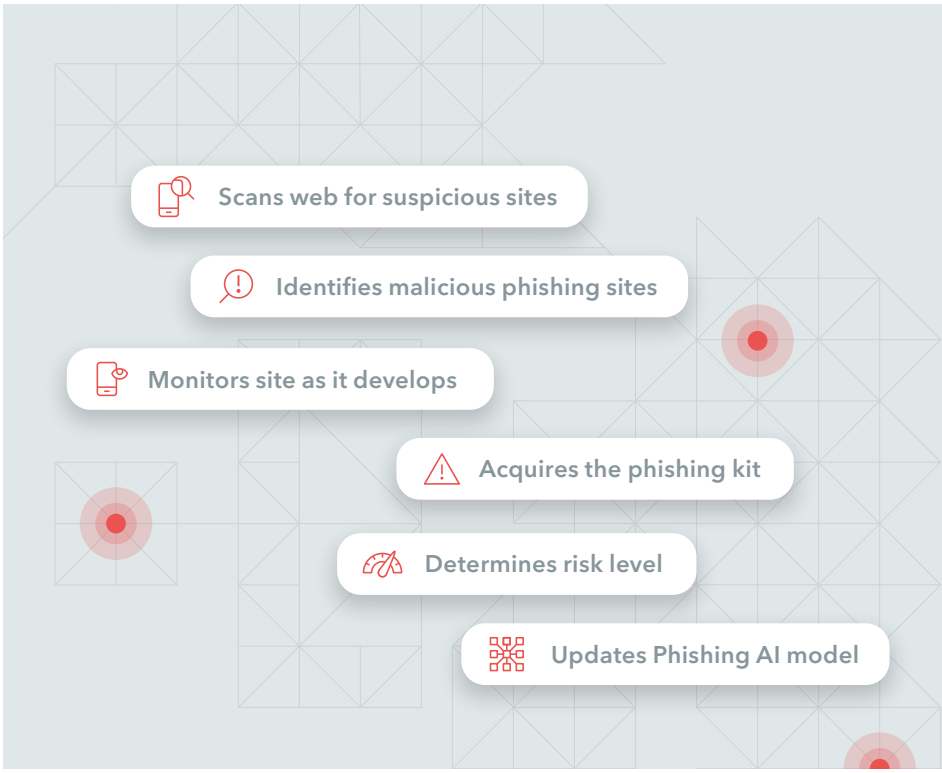
Lookout Phishing AI actively detects early signals of phishing sites and alerts organisations

Overview

Most cyber attacks targeting the enterprise begin with phishing. There are fewer ways into the enterprise faster than using stolen credentials to access sensitive data. To combat this, Lookout developed Phishing AI to identify early signals of attacks, build protections for our customers, and provide early warning to any targeted organisations – regardless of whether they are Lookout customers or not. With the ability to identify phishing tools as they are being built across the internet, Lookout Phishing AI often notifies targeted organisations before a phishing attack has started. We also share selected findings with the world on Twitter, here @PhishingAI.

How it works

Armed with sophisticated artificial intelligence, Phishing AI leverages patented pattern recognition technologies and machine learning to actively search the internet for precursors of phishing sites. Upon initial detection of potential phishing site infrastructure, Lookout AI deploys agents that extract features from servers to generate risk scores, creating powerful data sets based on the results of interacting with billions of sites. The machine learning engine not only monitors the phishing kit as it is initially being developed, but also continues to monitor the kit throughout its evolutionary life cycle. Phishing kits rapidly emerge, attack, and disappear, only to re-emerge later with different exploit capabilities. Due to the ever-changing nature of phishing kits, Lookout AI remains persistent to stop attacks before they reach users.



Capability highlight

Computer vision

One technique that Phishing AI uses is computer vision, which allows Lookout to identify the difference between valid sites and malicious copies of the sites that users enter their credentials into every day. Using computer vision, Phishing AI is able to analyse the use of logos and graphics to identify even the most sophisticated phishing sites. As phishing gains in prominence, attackers are creating impressive copies of sites, making it very difficult for humans to spot a malicious site.

Why is Phishing AI needed to stop attacks?

Phishing AI detects and tracks over 10,000 active phishing sites each day. This global criminal phenomenon is happening at such a speed and scale that humans can't identify, react, and remediate these threats in real time quickly enough to be effective. Phishing works at an international scale, reaching across multiple jurisdictions. This makes it nearly impossible for any one governmental organisation, let alone any human, to take effective action. Only an AI-based approach can effectively detect and combat criminals around the world that are constantly evolving their approach to tricking billions of internet users into falling for phishing attacks.

Why Lookout

Extend your phishing protection to mobile by adding a powerful line of defence against phishing attacks across personal email, texts, messaging platforms, and apps.

Accelerate digital transformation by confidently embracing the use of mobile devices for work and protecting against malicious content whether the employee is inside the protected corporate network or not.

Comprehensive protection at scale across the entire spectrum of mobile risk including the web and content threat vector, one of the most prevalent mobile vectors used by attackers to exfiltrate enterprise data.

Phishing highlights

- Phishing AI detects and tracks over 10,000 active phishing sites every day.
- Phishing AI is discovering 500 new high-confidence phishing sites every day.
- Enterprise users are three times more likely to fall for a phishing link on mobile.

Mobile phishing (60%) is reported as a more frequent mobile security incident than physically lost/stolen devices (30%)[1]

[1] IDC 2019 Mobile Security and the Future of Work; Phil Hochmuth

The Lookout difference

- Lookout has amassed one of the world's largest mobile security datasets due to our global scale and mobile focus. Lookout has collected security data from over 170 million devices worldwide and over 70 million apps, with up to 90,000 new apps added daily.
- This global sensor network enables our platform to be predictive by letting machine intelligence identify complex patterns that indicate risk. These patterns would otherwise escape human analysts.
- Mobile is a new era of computing and requires a new era of security solution designed exclusively for this platform. Lookout has been securing mobility since 2007 and has expertise in this space.

Lookout empowers your organisation to adopt secure mobility without compromising productivity by providing the visibility IT and security teams need. To learn how you can secure your mobility fleet today, contact us at lookout.com/uk.