How Lookout Phishing and Content Protection Works

Understanding phishing and content threats on mobile

Phishing is the primary means an attacker is going to use to gain access to your organization's network. It is relatively easy to fool an end user into clicking on a link, which can lead to malicious websites or downloads. In fact, Lookout exclusive data indicates that up to 29% of employees are fooled into clicking links during phishing tests. Attackers have discovered that email is the lowest cost method to execute a phishing attack. Many organizations have already invested in email security protections delivered via firewalls, gateways or spam filters, which is useful in also stopping phishing attacks on mobile when devices are used for work email purposes only. However this is increasingly unrealistic as employees are able to access corporate and personal email, and corporate and personal apps, all on the same device.

Phishing is both different and more problematic on the mobile device, as it presents new channels for phishers to deliver attacks beyond corporate email including:

Personal email – a phishing email can be sent to a personal email account, which bypasses the commodity security protections in place on many free email services and tricks the user into clicking on a link which then compromises the data, and corporate access, on the device

SMS text messages – a text sent to an unsuspecting user containing a shortened link that leads to a malicious website or triggers the download of a malicious app or surveillanceware

Malicious ad networks – domains are embedded into mobile apps to communicate with other services and provide richer experiences for users – such as providing directions, connecting to shopping sites or displaying contextually relevant ads. However if an app is programmed to access a malicious domain, that may trigger the download of plug-ins for malware or spyware.

Messaging platforms – a message sent to a user via WhatsApp, Facebook Messenger or Instagram to lure users to download spyware

Why enterprises need to protect against mobile phishing

According to IDC, over 51% of organizations reported employees had been targeted by mobile email phishing attacks in 2020[1]. In fact, 29% of Lookout users received and tapped a phishing domain on their personal mobile device. Of these users, 43% tapped more than three phishing domains on their devices in the course of a year[2].

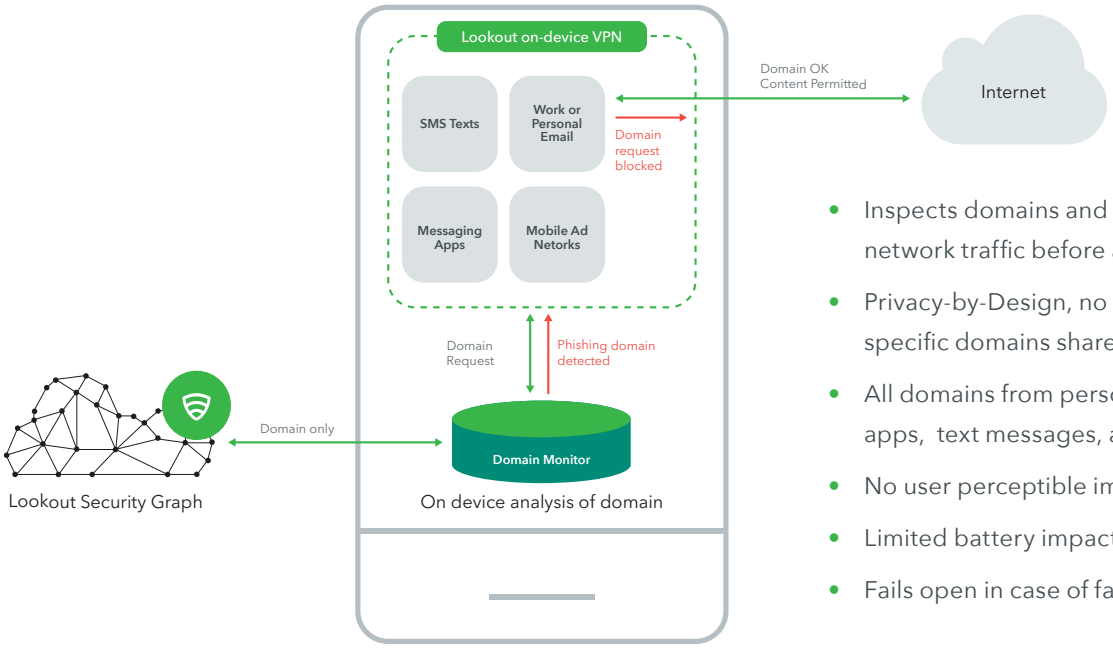
The rate at which Lookout users are tapping malicious domains on mobile devices has increased an average of 85% per year since 2011.

[1]Source: IDC 2018 U.S. Enterprise Mobility Decision Maker Software Survey

[2]Source: Lookout exclusive data, January 1, 2020 to December 31 2020

How it works

Lookout artificial intelligence engines protects the enterprise from both zero-day and known cybersecurity threats, as well as real-time detection of phishing attacks. Lookout Phishing AI crawls the Internet looking for the creation of new phishing sites. With an always on, always looking approach, Lookout detects these malicious websites as they are being built, before attacks, before any user is targeted.



- Inspects domains and domain names in network traffic before access is granted
- Privacy-by-Design, no content inspected, or specific domains shared with enterprise admin
- All domains from personal and work email apps, text messages, and messaging platforms
- No user perceptible impact on performance
- Limited battery impact
- Fails open in case of failures

On the device, Lookout Phishing and Content Protection inspects any domain requests from email (corporate or personal), SMS texts, messaging apps, and embedded in app browsers, dynamically blocking requests for websites identified by Lookout as malicious.

Lookout Phishing and Content protection uses a locally hosted VPN to analyze traffic and detect when a browser or app on a device attempts to access a suspicious domain. To ensure user privacy, only the existence of an issue and the number of detections are reported to the MES Console. Administrators cannot view a device's browsing history or traffic through this feature. In the Lookout for Work app, this feature is referred to as "Safe Browsing."

Privacy and data collection

Lookout takes a Privacy by Design[2] approach in developing our products. We collect only the data that is necessary to deliver on our security value; we ensure that data is protected in-transit and at-rest; we do not collect inoffensive domains; and we have robust privacy controls to further limit the personal data that we collect and display to administrators.

To establish end user trust and to maintain regulatory compliance, Lookout is committed to achieving the highest levels of certifications and approvals. Our compliance initiatives include:

- FedRAMP JAB P-ATO – completed in April 2020
- ISO 27018 – completed in December 2017
- ISO 27001 – completed in June 2017
- GDPR – complies with the GDPR Regulation (EU) 2016/679

[2] https://en.wikipedia.org/wiki/Privacy_by_design

Focus on domain analysis

Lookout Phishing and Content Protection leverages a combination of on device and cloud-based, AI driven, analysis of domains that are requested from email, SMS messages, ad networks, and messaging platforms. No content from these apps is collected, stored, or shared with enterprise admins. No traffic or content is redirected off the device or through a web gateway of any kind.

Lookout's commitment to GDPR

General Data Protection Regulation (GDPR) imposes new rules on the protection of EU resident information as it pertains to privacy. Lookout takes every commercially reasonable effort inclusive of recommended technical and organizational measures to comply with GDPR (Regulation (EU) 2016/679).

GDPR contains requirements about how an organization should collect, store, use, and secure personal information. We focus on the following high-level requirements that align with GDPR compliance.

Why Lookout

Extend your phishing protection to mobile by adding a powerful line of defense 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.

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 nearly 200M devices worldwide and over 140M apps, with up to 100K 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 organization to adopt secure mobility without compromising productivity by providing the visibility IT and security teams need. To learn how you can secure your mobile fleet today, contact us at lookout.com.