Lookout

LOOKOUT MOBILE PHISHING AND CONTENT PROTECTION

VISIBILITY AND PROTECTION AGAINST A MASSIVE THREAT ON A SMALL SCREEN

Mobile phishing is the biggest threat to all modern endpoints

Mobile phishing is one of the most critical threats for organizations across all industries and geographies. We trust our mobile devices. Whether they are company- or employee-owned, we treat them as an integral part of both our personal and professional life. We take photos of our friends and family, we communicate with colleagues, and log onto business applications. Mobile devices today provide the same access to business data as laptops and desktops.

Unlike our desktop, there are endless ways for cyber attackers to deliver phishing links via iOS, Android and Chrome OS apps. They can send us a phishing link in virtually any app on our device. These include social media, messaging, gaming, and even dating apps. Lookout research shows that 1 in 50 enterprise users are phished on mobile devices daily.

The majority of mobile phishing attacks now start outside of email in SMS, social media, gaming, or third-party messaging platforms. In addition, an attacker can socially engineer a target through mobile apps, tricking them into giving up both personal and corporate data.

KEY STATISTICS

- 1 in 50 enterprise users are phished on mobile endpoints daily
- Corporate mobile devices are 50% more susceptible to mobile phishing than BYOD
- Mobile phishing rates are double for users of Office 365 and G Suite
- 1 in 3 phishing attacks intend to steal credentials

A phishing attack can come from anywhere

The design of mobile interfaces obfuscates details typically available on a desktop that can help us identify a phishing attack. Mobile URLs are truncated and we can't hover over links to expose the full URL or email address. This means there is a greater imperative to have phishing protection on mobile devices.

Using traditional anti-phishing approaches on mobile devices quickly becomes a privacy issue because they inspect email messages to block attacks. All mobile

devices, even if company issued, are considered to be a personal device. Only inspecting email content would miss the other 99% of methods used for sending a phishing link to a mobile user.

Many organizations have already invested in email security protections, but lacking protection against these additional threats on mobile, they are leaving a significant gap in their security posture. These include personal email, SMS, malicious ad networks and messaging apps.

Most anti-phishing solutions rely on a list of nefarious domains and web addresses. However, more than 1.5 million mobile phishing sites are created every month. And most phishing sites are built and dismantled in a matter of hours or days. Relying on reputation-based methods to detect a mobile phishing attack alone is insufficient.

Delivering 360-degree phishing and content protection for mobile

360-degree phishing protection

Lookout phishing and content protection stops both known and unknown phishing threats. We combine our Phishing AI engine with reputation lists of known phishing sites. This engine continuously monitors for the establishment of new websites purpose-built for phishing. Phishing AI enables Lookout to provide near real-time protection against zero-day phishing attacks.

We compare every web request from your mobile device with this combined dataset. This comparison is made for all the network interfaces of your mobile device - Bluetooth, Wi-Fi, and cellular. By performing the comparison on the local device rather than sending it to the cloud, we are respecting the individual's privacy. The result is 360-degree protection from known and unknown phishing attacks.

Content protection via web filtering

With the same technique used to analyze web requests for phishing protection, we can also block inappropriate content from being presented to employees. Lookout web content filtering enables you to extend existing content and acceptable-use policies for laptops and desktops to all mobile devices being used for work.

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 that 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 – URLs 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 URL, 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.

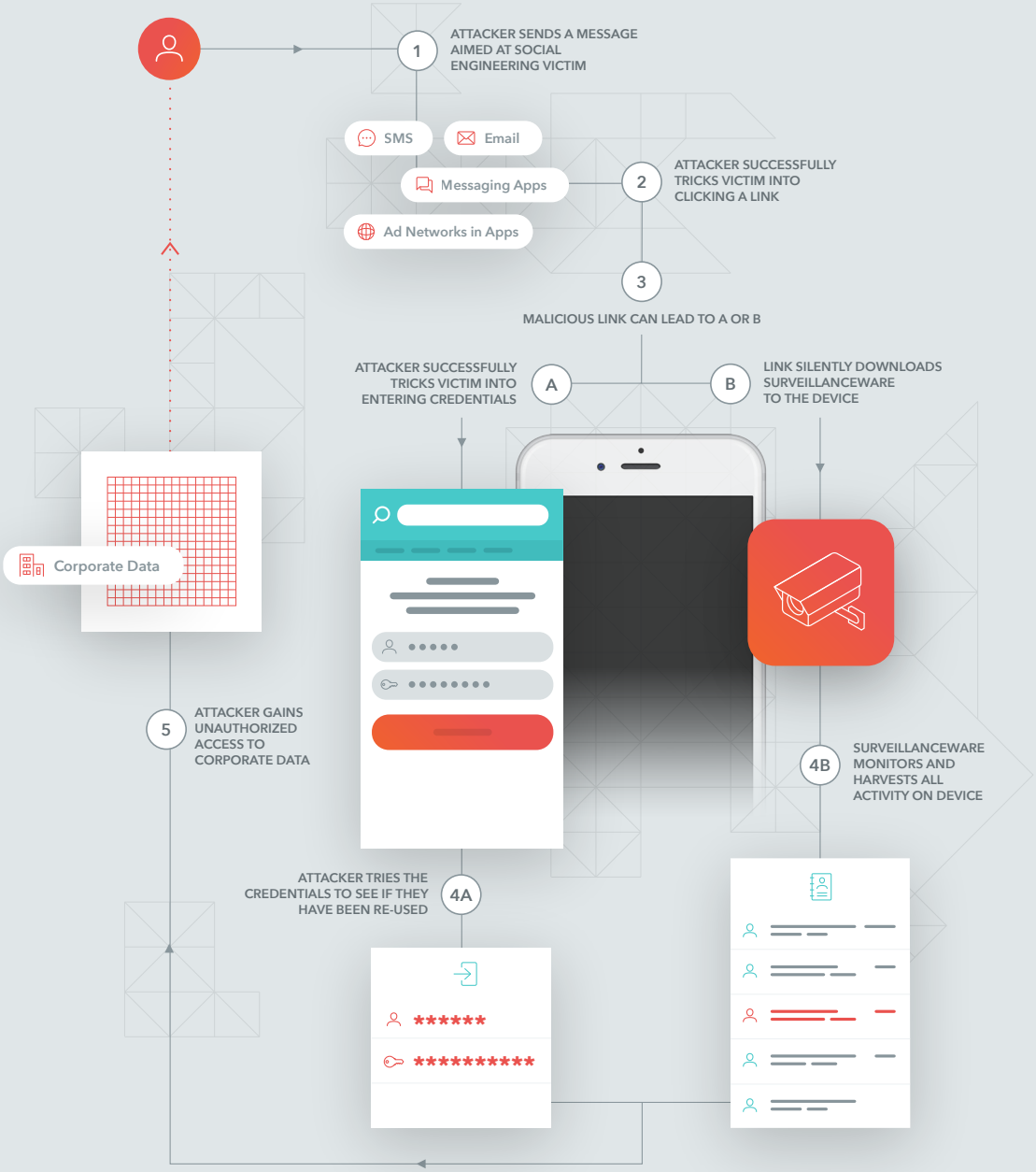
How Phishing Protection works

Lookout Phishing Protection stops cybercriminals from exploiting the small form-factor of mobile devices in order to phish your employees. By analyzing 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 maintains a dynamic cache of known malicious sites on the device based on its recent URL requests. Efficiency is maximized by checking that cache before going to the cloud to determine if a URL request is malicious. This hybrid approach creates the most efficient solution and optimizes the user experience and device battery life.

With Lookout Phishing Protection, you can confidently embrace the use of mobile devices as part of you digital transformation strategy. Lookout phishing protection works regardless of the network – cellular, bluetooth, corporate wifi, as well as their home networks.

The five links in the mobile phishing kill chain

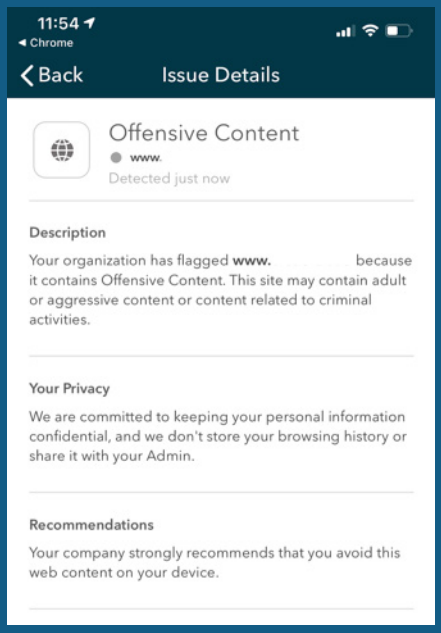


How Content Protection via Web Filtering Works

Lookout blocks access to inappropriate content on iOS and Android devices by inspecting outbound connections made by the mobile device and apps. We correlate the site being accessed against known violent, criminal, or adult content, and prevent connections in real time.

Admins can also implement custom filtering policies based on country-specific top-level domains (TLDs).

You can upload custom lists of sites to block, including video streaming sites, assign risk levels (e.g., high, medium, and low) and define response workflows. By doing this without inspecting content, Lookout preserves employee privacy and continuously limits exposure to risky content, enabling your team to extend existing content policies to all mobile devices.



Detail provided to the employee in the Lookout for Work app

What you should expect on your device

When Lookout blocks offensive or unapproved content, you can expect the following:

1. Depending on your organization's policy, employees will receive one of two types of notifications;

   Notification 1: content has been blocked and the user cannot access that content

   Notification 2: content is offensive, but the user can still choose to proceed to access the content. This will temporarily allow access to the URL before blocking it again.

2. Employees can view notification details, which includes a description of the blocked content, recommendations, and a note about privacy. They can also view a log of blocked URLs their device has tried to access.

3. Admins can view additional statistics related to your safe browsing experience, but by default cannot see the actual URLs in order to preserve employee privacy.

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

For more information visit **lookout.com**

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

A platform built for mobile from the ground up

Explore the Lookout Platform at **lookout.com/platform**

Lookout®