Lookout phishing and content protection

Understanding phishing and content threats on mobile

Phishing is the primary means an attacker is going to use to gain access to your organisation'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 25% 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 organisations 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 – 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.

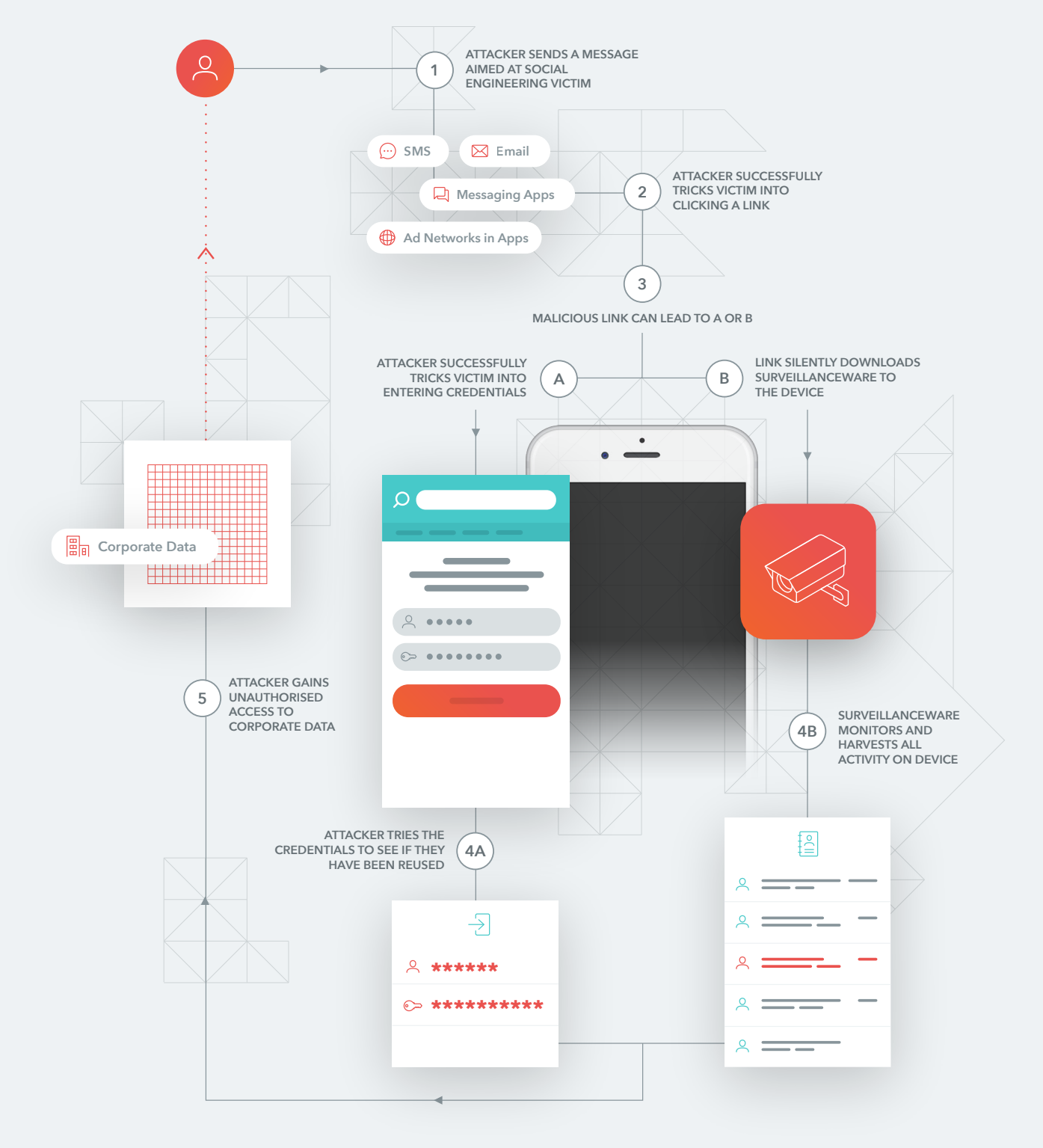
Messaging platforms – a message sent to a user via WhatsApp, Facebook Messenger or Instagram to lure users to download spyware

Security best practices to deter phishing and content threats

1. Ensure proper desktop and web gateway security is in place for corporate email accounts to avoid infections from malicious attachments and URLs.
2. Deploy comprehensive protection against mobile phishing on Android and iOS devices to cover personal email, SMS texts, messaging platforms and mobile apps.
3. Implement internal employee training on how to identify phishing and social engineering attacks across multiple channels including email, text and social media.

What is a phishing attack on mobile

Attackers are moving beyond email and mobile devices have quickly become a primary vector for phishing attacks to deliver surveillanceware and gain access to corporate data and networks.



Why enterprises need to protect against mobile phishing

Mobile users are three times more likely to fall for phishing scams, according to IBM. In fact, 56% of Lookout users received and tapped a phishing URL on their mobile device. These users tapped an average of six phishing URLs on their devices in the course of a year.

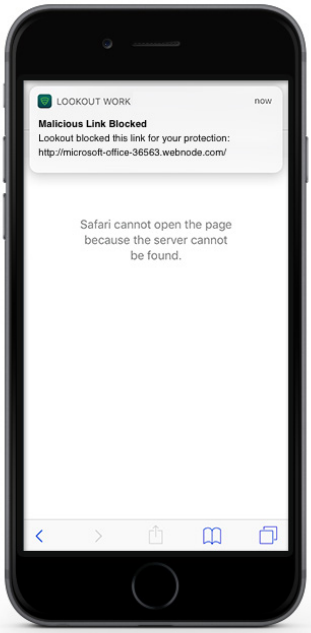
85% The rate at which Lookout users are tapping malicious URLs on mobile devices has increased by an average of 85% per year since 2011.

If an attacker is successful in tricking a user into providing corporate credentials, the attacker can then gain access corporate systems and move unchecked through your infrastructure and your data.

How Lookout protects against phishing attacks

Lookout phishing & content protection, a comprehensive feature in Lookout Mobile Endpoint Security, is designed to protect enterprises from phishing attacks from any channel, including email (corporate or personal), SMS texts, messaging apps and URLs embedded into apps.

Lookout inspects all outbound connections made by the mobile device and installed apps at the network level at the time a user attempts to connect. What is different about this approach is that it does not rely on inspecting message content, and therefore does not violate end user privacy. Lookout correlates the URL being accessed against known malicious URLs identified by the Lookout Security Cloud, and alerts the end user if it is malicious prior to the connection being completed. This real-time alert prevents exposure to risky content such as malicious apps or websites with known vulnerabilities.



Through the Lookout console, admins can block users who are attempting to make connections on mobile to known malicious URLs hosted on risky websites that may attempt to extract credentials.

Malicious URLs include ad fraud, botnets, command and control centres, compromised and links to malware, malware call-home, malware distribution points, phishing/fraud, spam URLs and spyware.

Admins can also opt to warn users of risky websites before proceeding. If phishing and content protection is disabled on a user's device, admins have the ability to mark the device out-of-compliance until protection is turned back on.

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.

The Lookout Difference

- Lookout has amassed one of the world's largest mobile security datasets due to the success of our consumer product. Lookout has collected security data from over 150 million devices worldwide and over 50 million apps, with up to 90 thousand 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 mobile fleet today, contact us at info@lookout.com