Lookout Stops Phishing Attacks Targeting Law Firms

Lookout Phishing and Content Protection protects attorneys from mobile threats

Industry-Wide Security Challenges

Law firms are highly dependent on mobile devices, which allowing attorneys to be responsive to client needs. This means a large amount of information they are required to keep private and confidential is accessed outside the four walls of a firm, and outside the reach of traditional security tools. The need to work at any time and from anywhere means devices are used for personal and work life, which often results in a conflict between security and privacy for attorneys. A mix of personal and corporate-owned devices also poses a significant challenge for law firms, particularly as more customer data is stored in cloud-based services.

Real World Use Case for Law Firms

Attorneys are a prime target for mobile phishing attacks as they rely on mobile devices, but law firms oftentimes have legacy secure models in place. In fact, 80% of law firms reported phishing attempts in 2018[1]. The goal of attacks is to capture corporate cloud credentials to get to sensitive client information, so IT and security teams must be able to provide security tools that identify phishing links on mobile devices across work and personal email, messaging, and social media applications.

Industry Challenges

1. Significant adoption of mobile devices for all firm employees
2. Protecting sensitive client PII and case documentation
3. Wider mix of work and personal apps increase the risk of mobile phishing through messaging and social platforms.

Lookout Critical Capability

Lookout Phishing and Content Protection inspects any URL requests, including corporate and personal email, SMS, messaging apps, and Apps containing URLs that download malicious plug-ins. Lookout dynamically blocks URL requests for websites identified by Lookout as malicious. For example, with this feature enabled, Lookout would prevent a phished employee from potentially entering login credentials to a malicious replica of an Office 365 login page. Additionally, to ensure user privacy, Lookout only reports the existence of an issue and the number of detections to the Mobile Endpoint Security Console. Administrators cannot view browsing history or traffic.

Why Lookout

Lookout Mobile Endpoint Security with Continuous Conditional Access ensures security and compliance on every device, leveraging a large data set fed by over 170 million devices and the analysis of over 70 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide conditional access to sensitive corporate applications and data.

[1] National Cyber Security Centre: https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report