Secure your legal practice from mobile threats

Empower your attorneys to securely telecommute

Industry-wide security challenges

Mobile devices enable your attorneys and staff to telecommute from anywhere. But this has also introduced risks into your law firm. Because work and personal lives are converging on these devices, your attorneys have become easy targets of phishing attacks. These phones and tablets may also be carrying apps that could violate privacy or compliance requirements. With everything so interconnected, a well-placed phishing attack or a risky app could compromise your firm's data.

Real world use case for law firms

Being always on the move, attorneys use their mobile devices with speed and efficiency. But that means they are also susceptible to phishing attacks, especially when the smaller screen and countless apps enable cyberattackers to deliver socially engineered attacks. The goal of these attacks is often to capture corporate cloud credentials to get to sensitive client information. Lookout Phishing and Content Protection uses artificial intelligence to automatically stop known and unknown phishing attacks, providing 360-degree protection.

Industry Challenges

1. Significant adoption of mobile devices for all firm staff
2. Protecting sensitive client PII and case documentation
3. Mix of work and personal apps increases 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.

About Lookout

Lookout Mobile Endpoint Security with Continuous Conditional Access ensures security and compliance on every device, leveraging a large data set fed by nearly 200 million devices and the analysis of over 120 million mobile apps. With the Lookout Security Platform, 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 Continuous Conditional Access to sensitive corporate applications and data.