Lookout

Mobile Threat of the Month

June 2025

The Human Factor: The Weakest Link

Cybercriminals have adapted by shifting from traditional malware to sophisticated social engineering campaigns that target human vulnerabilities to steal user credentials. This credential theft often initiates the "modern kill chain", which centres on the human factor becoming the weakest link in security, especially with the rise of social engineering attacks that exploit human instincts like trust and curiosity.

Historically delivered via email phishing, these attacks have evolved with AI into highly targeted omnichannel attacks, including SMS (smishing), voice calls (vishing), and sophisticated phishing websites. Mobile devices have become the primary vehicle for these attacks because they are always on, widely used, and closely connected to users' lives.

Social Engineering Effectiveness

Socially engineered mobile cyberattacks draw on common tactics that are highly effective:

Mobile Convenience: The attack leverages the convenience of mobile devices, where users are often more likely to click on links and may not scrutinise URLs as closely as they do on a desktop.

Urgency: The message implies a time-sensitive issue ("urgent," "delayed," "immediate action") that creates a sense of panic and bypasses critical thinking.

Curiosity: People are naturally curious about a clickable link, especially if the nature of the message appears relevant and of interest.

Trust: Users generally trust well-known reputational brands or even employees or individuals who are being impersonated, making them less suspicious.

Emotional Manipulation: The resulting impact of not following through with the required action can lead users to act impulsively

Lookout Mobile Security

Lookout detects and remediates coordinated social engineering attacks that exploit human behaviour using the world's largest AI-driven mobile security dataset. This includes detecting socially engineered phishing attacks that originate from suspicious SMS messages, executive impersonation or users clicking on suspicious links across messaging apps on iOS, Android and ChromeOS devices.