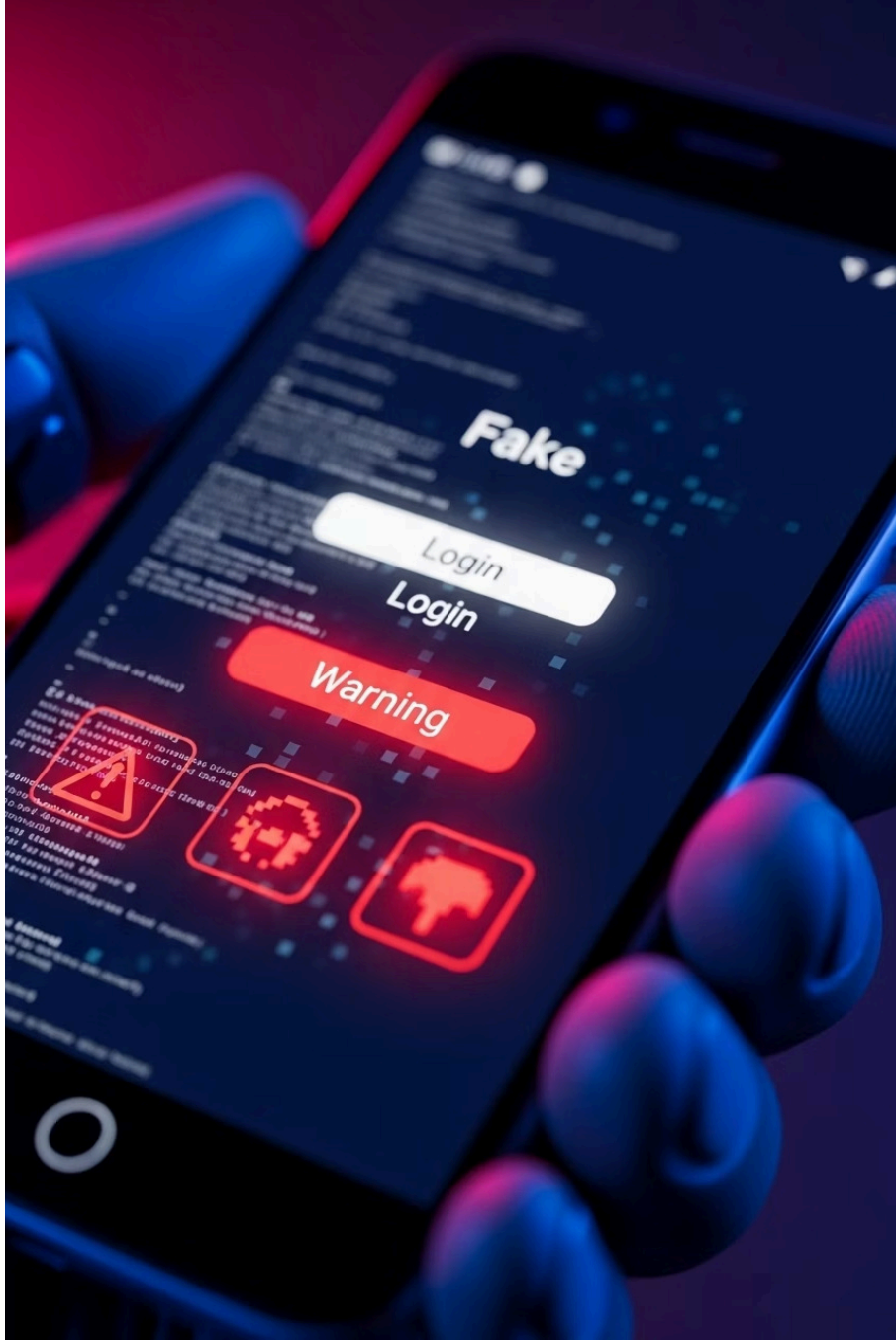
Web, Network & Social Engineering Attacks on Android in 2025

This presentation explores the evolving landscape of Android security threats in 2025, examining web-based, network-based, and social engineering attack vectors. We'll investigate current trends, analyze real-world case studies, and provide actionable defensive strategies for organisations to protect their Android users and infrastructure.



Chapter 1

The Rising Tide of Android Threats

The Android ecosystem faces unprecedented security challenges in 2025. As businesses increasingly rely on mobile technology for critical operations, threat actors have intensified their focus on exploiting Android vulnerabilities through sophisticated attack vectors.

This rapidly evolving threat landscape combines technical exploits with psychological manipulation, creating a perfect storm of security challenges for organisations of all sizes.

Over 1 Million Mobile Phishing & Social Engineering Attacks in Q1 2025

1,088,406

Blocked Attacks

Lookout reports this massive number of phishing and malicious web attacks blocked on Android enterprise devices in just three months

100%

Enterprises Targeted

Every single protected enterprise faced social engineering phishing campaigns targeting their Android users

These figures represent only detected and blocked attacks, suggesting the actual number of attempts may be significantly higher. The universal targeting indicates that no organisation, regardless of size or industry, is immune to these threats.

Android Malware Surged 151% in Early 2025

151%

Overall Malware Increase

General Android malware attacks showing dramatic quarterly growth

692%

Smishing Explosion

SMS-based phishing attacks showing the most dramatic increase

147%

Spyware Growth

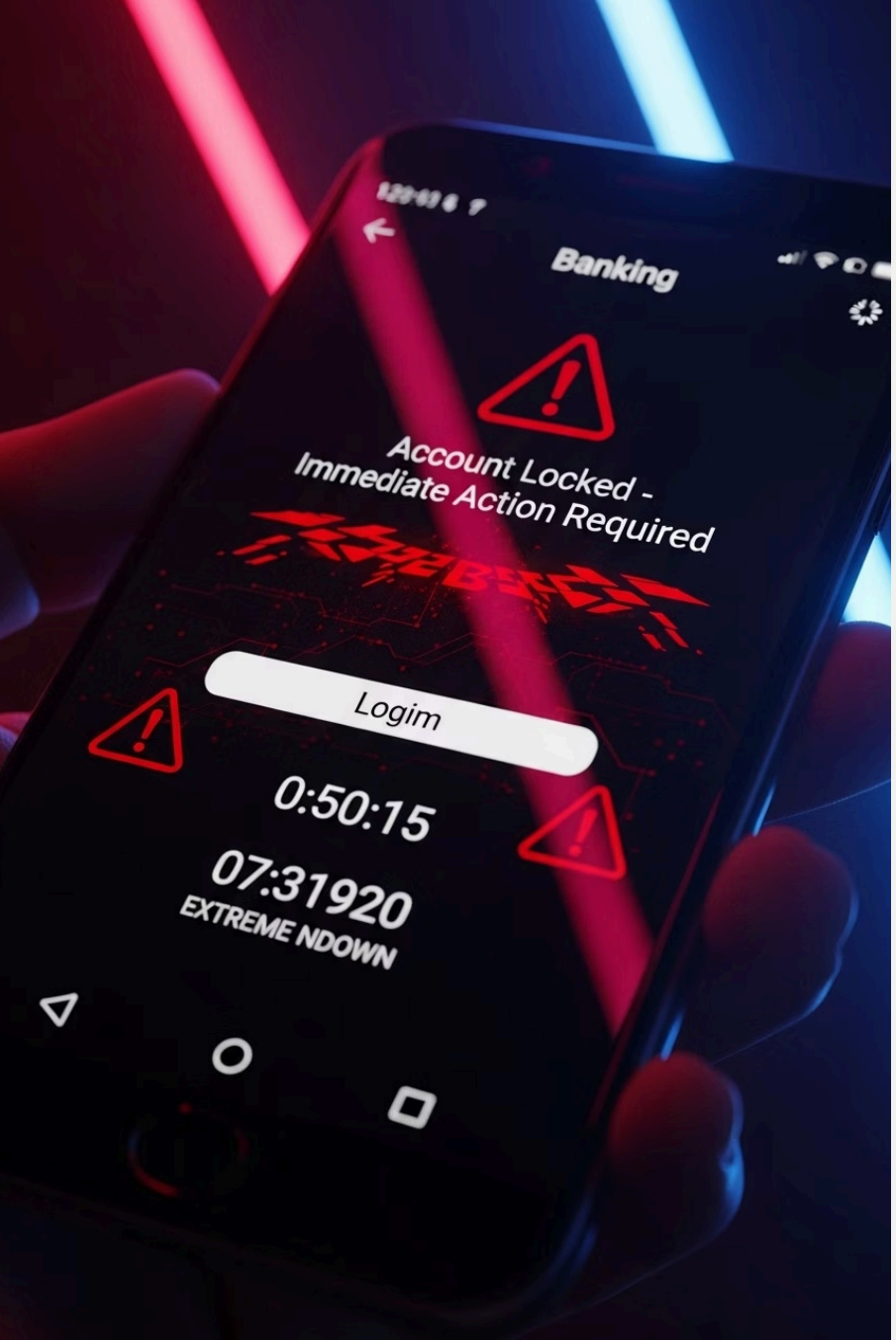
Privacy-invading surveillance tools targeting sensitive data

Seasonal Targeting

Attackers strategically time campaigns around:

- Tax filing deadlines
- Major holidays
- Financial stress periods
- Global events

Source: Malwarebytes Quarterly Threat Report, May 2025



Attackers exploit human psychology with urgent threats

This example shows how attackers create a false sense of urgency to bypass rational thinking. The fake banking notification leverages fear of financial loss to prompt immediate, unthinking action from the victim.

When users are emotionally triggered, they're 3.2× more likely to ignore security warning signs and comply with malicious requests.

Chapter 2

Web-Based Attacks on Android

Web-based attacks target Android users through malicious websites, compromised legitimate sites, and phishing pages. These attacks exploit browser vulnerabilities, social engineering, and increasingly sophisticated delivery mechanisms.

Browser Exploitation

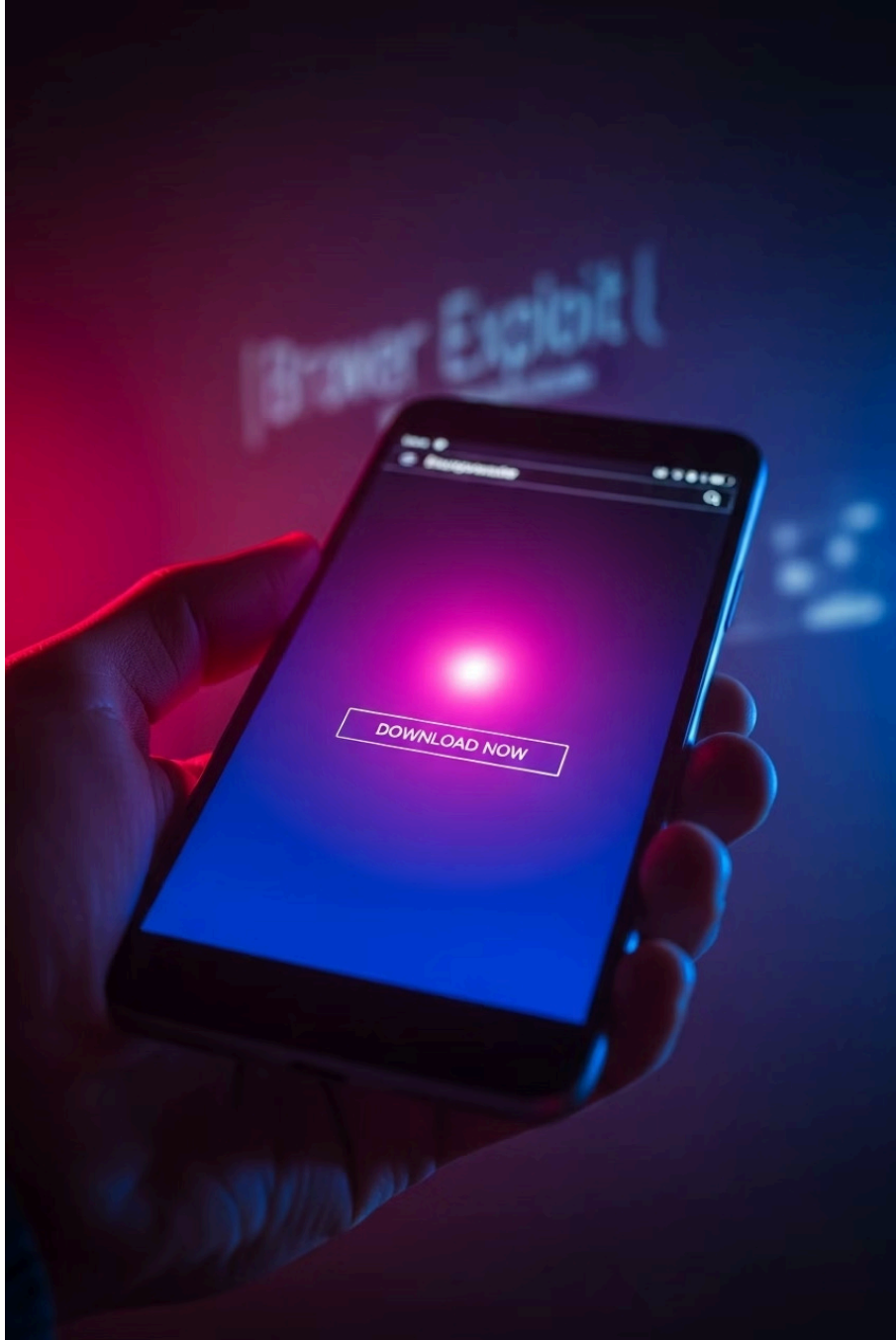
Attackers target WebView and Chrome vulnerabilities to execute malicious code

Drive-by Downloads

Malicious sites that automatically download malware without user confirmation

Credential Harvesting

Convincing fake login pages that steal authentication details

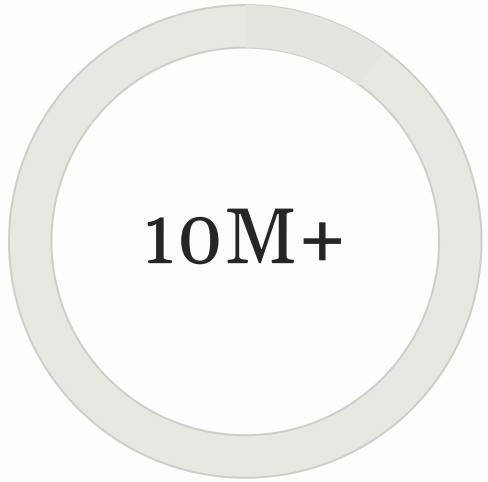


Mobile Phishing & PDF Phishing: The New Gateways

PDF phishing has emerged as a particularly effective attack vector, leveraging trusted document formats to bypass traditional security controls.

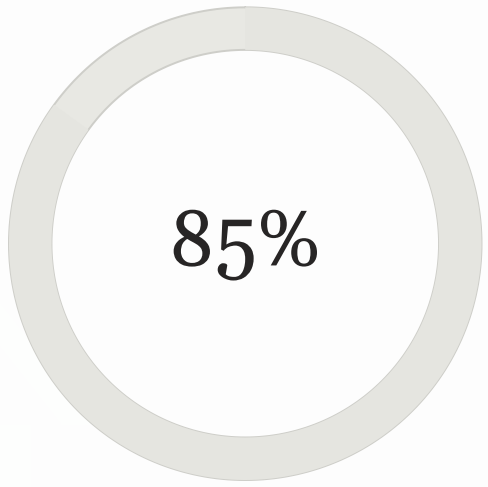
These attacks typically involve:

- Embedding malicious links in seemingly legitimate PDFs
- Creating convincing replica documents from trusted entities
- Exploiting Android PDF viewer vulnerabilities
- Using QR codes within PDFs to direct to phishing sites



Blocked Sites

Phishing and malicious websites blocked in Q1 2025 by Lookout alone



AI-Generated

Proportion of phishing lures using AI to craft convincing messages

⚠ AI-generated phishing messages have become virtually indistinguishable from legitimate communications, with spelling, grammar and contextual awareness that evade traditional detection methods.

SEO Poisoning & Fake Browser Prompts

SEO Poisoning

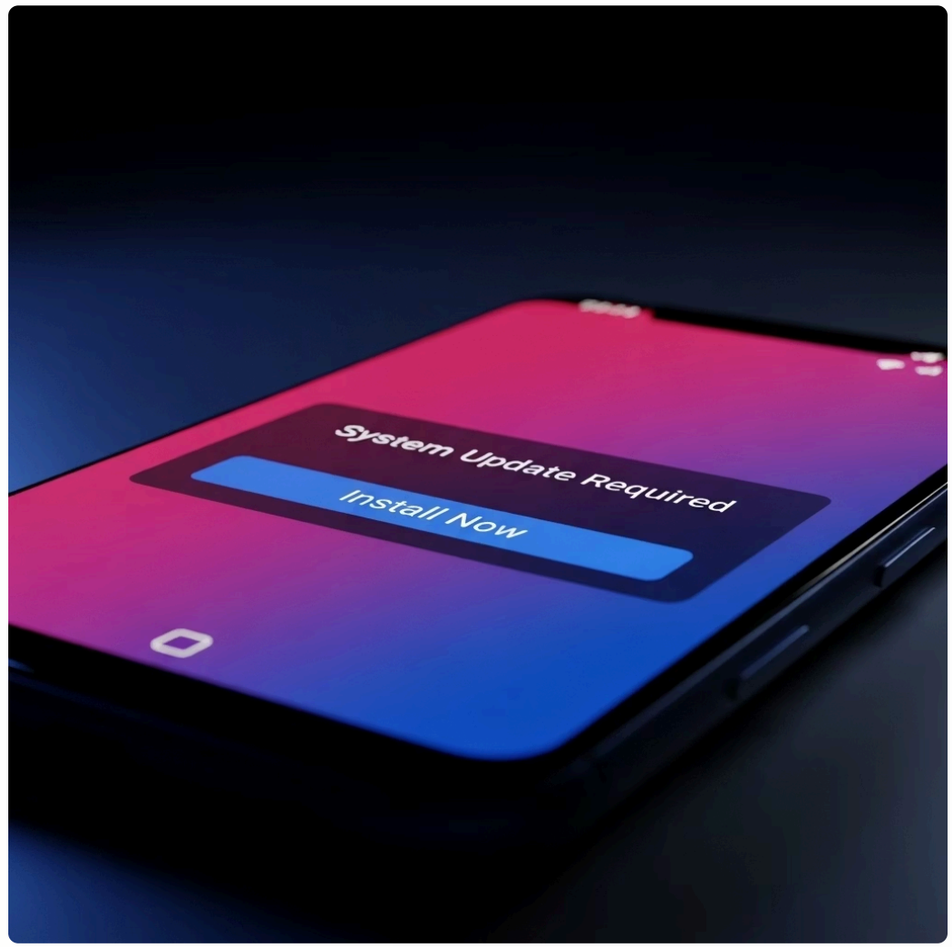
Attackers manipulate search engine results to position malicious sites prominently in results for common queries:

- Leveraging trending topics and news events
- Creating convincing fake review sites for popular apps
- Injecting malicious content into compromised legitimate sites
- Using AI to generate content that ranks well in search engines

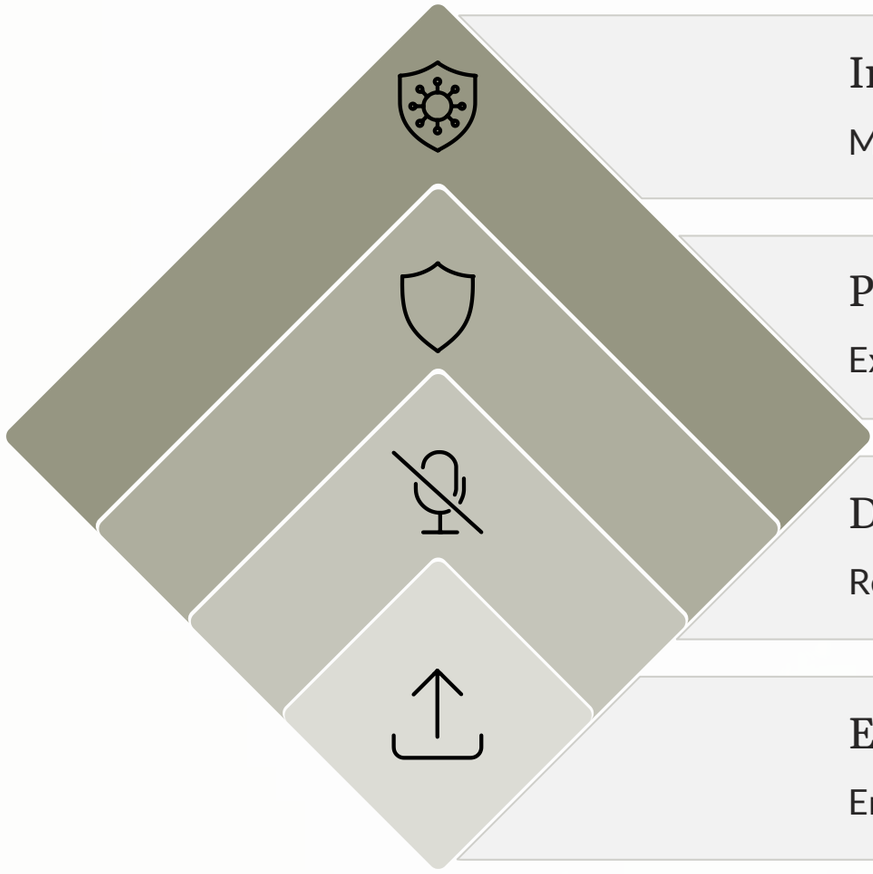
Fake Browser Prompts

These attacks mimic legitimate system dialogs to trick users:

- Fake "Update Required" messages
- Counterfeit security warnings
- Deceptive permission requests
- Browser notification prompts leading to malware



Case Study: KoSpy Android Surveillance Tool



Initial Infection

Malicious APK delivered via phishing

Privilege Escalation

Exploit kernel vuln or abuse root

Data Collection

Record audio, camera, SMS, location

Exfiltration & Persistence

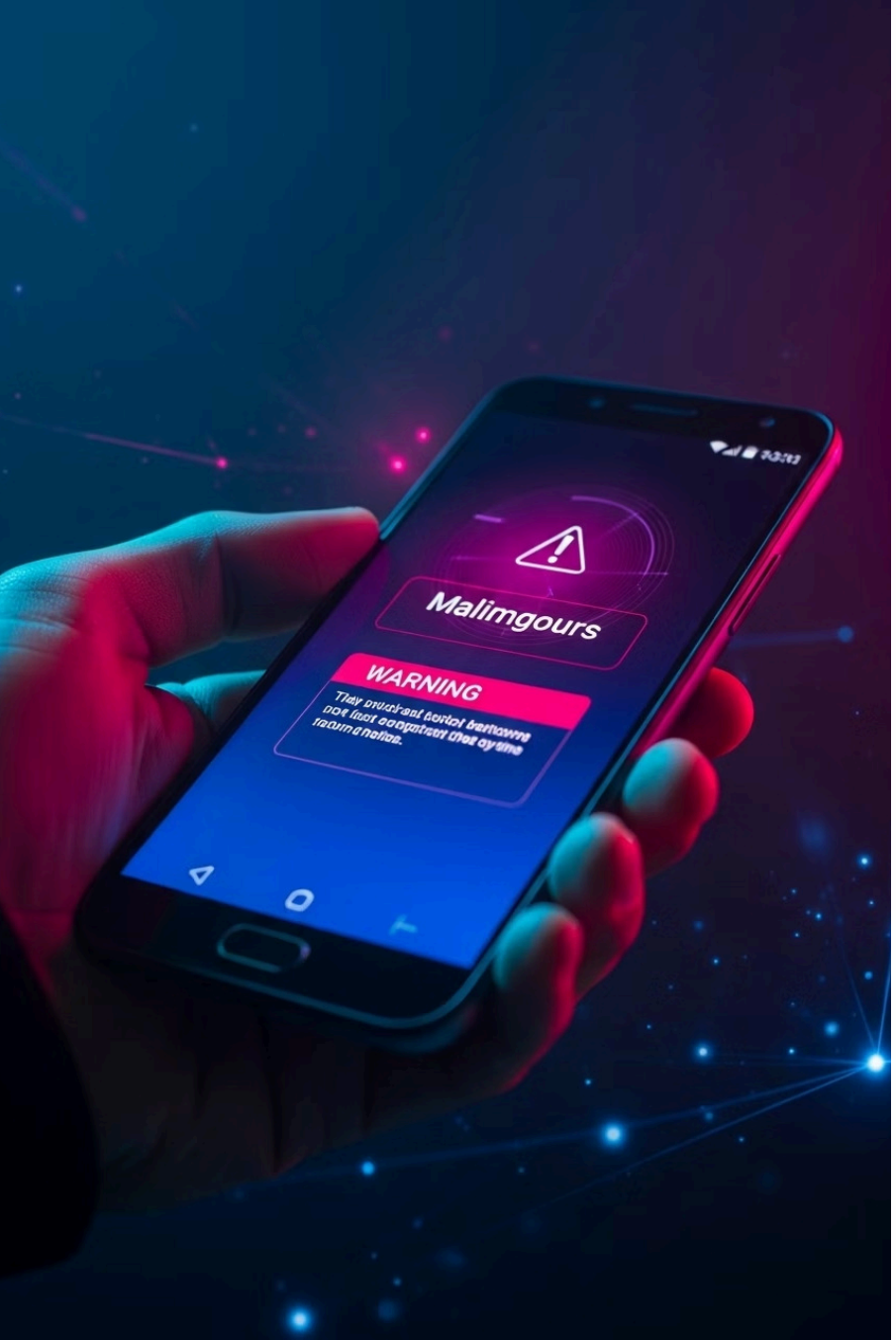
Encrypt, upload and install watchdog

Key Findings

- Discovered by Lookout security researchers in November 2024
- Linked to North Korean advanced persistent threat group ScarCruft (APT37)
- Primarily targets Korean and English speakers
- Active since 2022 with continued development
- Demonstrates growing sophistication of state-sponsored mobile attacks

Capabilities

- Call recording
- SMS interception
- Location tracking
- Media file exfiltration
- Contact theft
- Application data extraction



Chapter 3

Network-Based Attacks on Android

Network-based attacks target the communication channels Android devices use to connect to services and transfer data. These attacks exploit vulnerable network configurations, insecure protocols, and compromised infrastructure.

Wi-Fi Interception

Fake access points and man-in-the-middle attacks

Traffic Analysis

Passive monitoring of unencrypted data transmissions

Sideloaded Malware

Malicious apps installed outside of official app stores

Rogue Wi-Fi & Session Hijacking

Rogue Wi-Fi Attacks

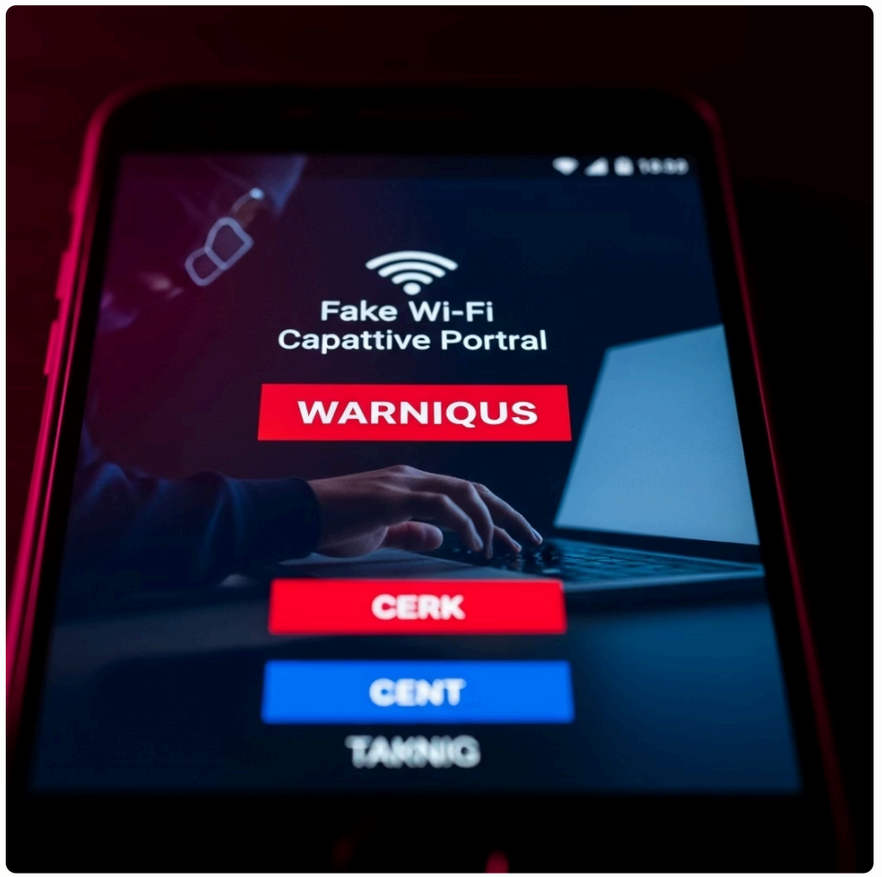
Attackers deploy counterfeit hotspots in public locations to intercept traffic:

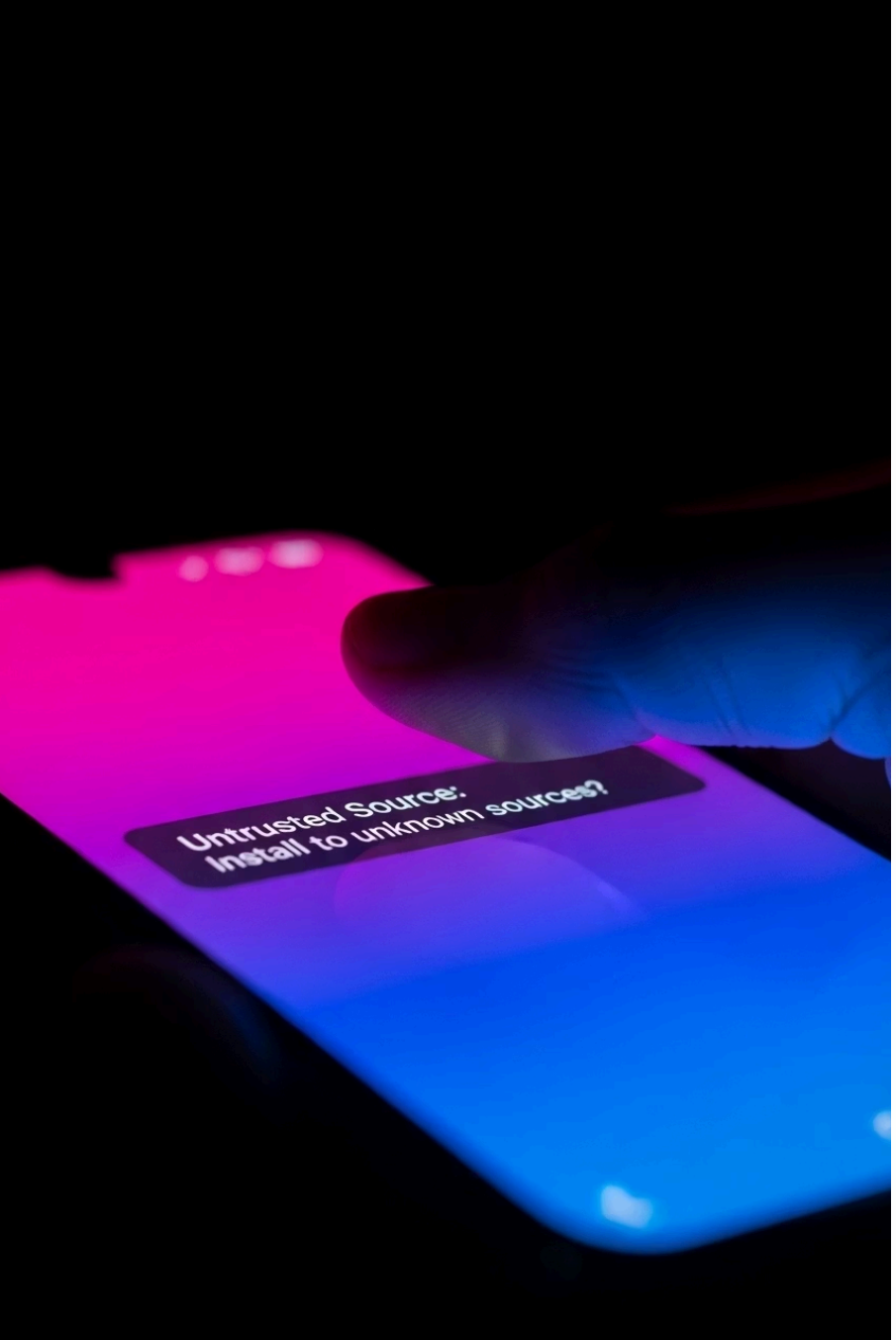
- Evil twin networks mimicking legitimate hotspots
- Captive portals that harvest credentials
- SSL stripping to downgrade encrypted connections
- DNS poisoning to redirect traffic to malicious sites

Session Hijacking

Attackers steal authentication tokens to compromise accounts:

- Sidejacking via unencrypted cookies
- Cross-site request forgery attacks
- Session fixation exploits
- OAuth token theft from compromised apps





Sideloaded Apps: A Hidden Danger

23.5%

Of enterprise Android devices have at least one sideloaded app installed outside of official app stores

41%

Of these sideloaded apps contain security vulnerabilities or actively malicious code

68%

Of Android malware infections in enterprise environments originate from sideloaded applications

Common Sideloading Vectors

Repackaged Apps

Legitimate apps modified with malicious code, often premium apps offered "for free"

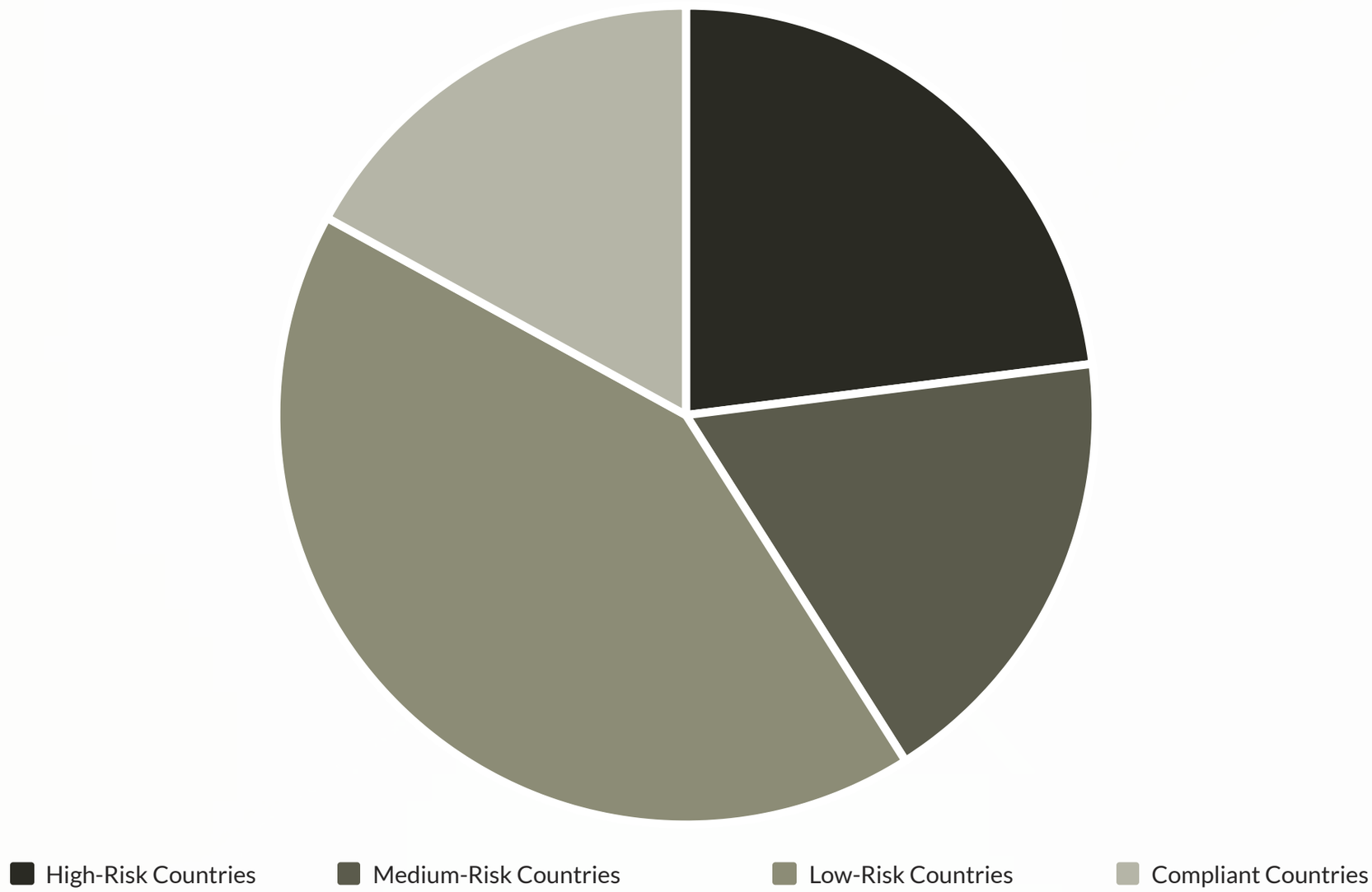
Alternative Stores

Third-party app stores with inadequate security screening

Direct Downloads

APK files shared via messaging apps, email, or direct links

Data Leakage via Risky App Communications



Nearly one-quarter of work-related Android applications communicate with servers in embargoed or high-risk countries, raising significant concerns about data sovereignty, regulatory compliance, and potential espionage risks.

This communication often occurs without user awareness or explicit consent, and frequently violates corporate security policies and data protection regulations like GDPR, creating both security and compliance liabilities.

Chapter 4

Social Engineering Attacks on Android

Social engineering attacks exploit human psychology rather than technical vulnerabilities, manipulating users into compromising their own security. On Android, these attacks blend technical elements with sophisticated psychological manipulation.

The human element remains the most exploitable vulnerability in mobile security, with attackers leveraging emotional triggers such as fear, urgency, curiosity, and trust to bypass rational decision-making processes and security awareness.

> While technical defences continue to improve, attackers increasingly focus on the psychological aspects of security, crafting increasingly personalised and convincing social engineering attacks.

Smishing: AI-Powered SMS Phishing on the Rise

The Evolution of Smishing Attacks

SMS-based phishing has evolved dramatically with AI integration:

- Natural language processing creates grammatically perfect messages
- Contextual awareness references relevant details like local banks
- Personalisation through data aggregation from multiple breaches
- Real-time adaptation to security awareness trends
- Psychological profiling to target vulnerable personality types

67%

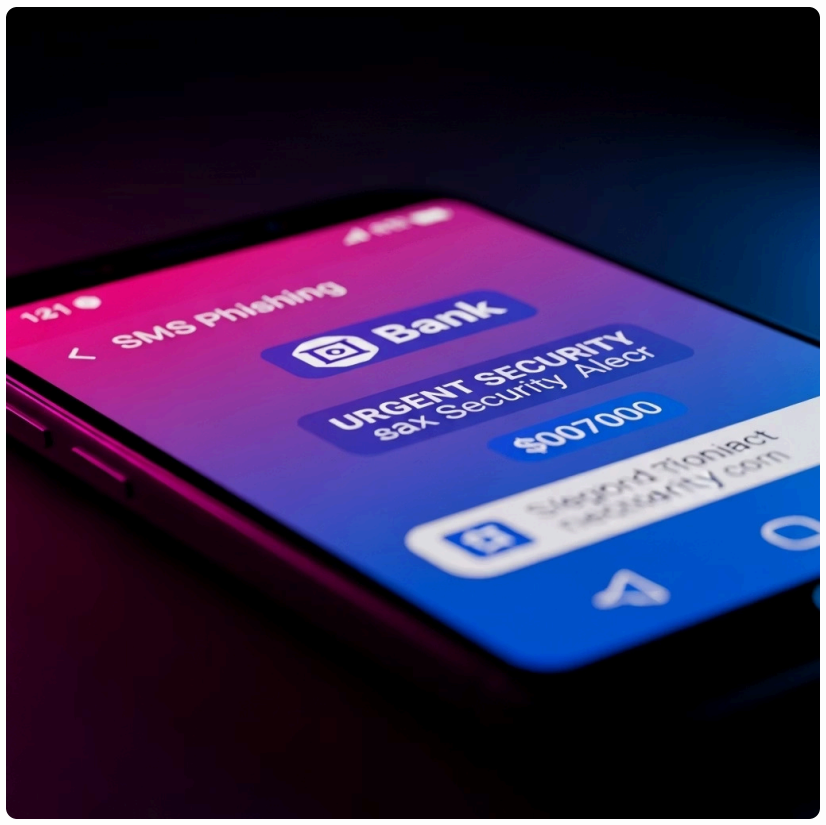
Mobile Phishing

Proportion of mobile phishing attacks delivered via SMS

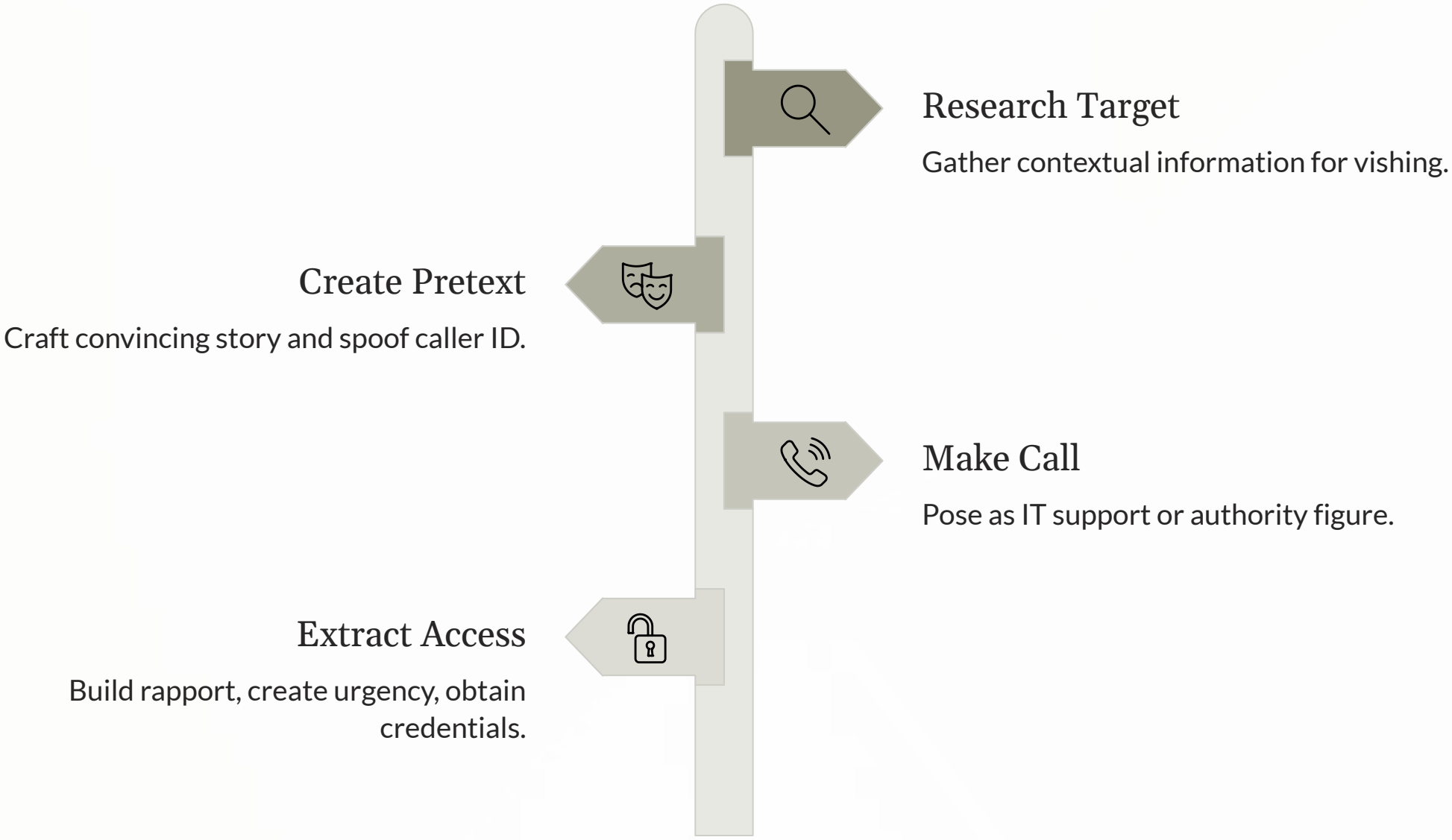
4.3×

Higher Open Rate

SMS messages are opened more frequently than email phishing



Vishing & Help Desk Manipulation



Case Study: Google Salesforce Breach (August 2025)

The ShinyHunters hacking group successfully breached Google's Salesforce database using a sophisticated vishing attack that bypassed multi-factor authentication:

1. Attackers called employees claiming to be from Google IT support
2. They referenced legitimate recent IT tickets to establish credibility
3. Victims were guided to a convincing fake Google login portal
4. The attackers captured both passwords and time-based one-time passwords
5. This allowed real-time session hijacking despite MFA being enabled

High-Touch Social Engineering Attacks

1 Live Impersonation

Real-time voice or video calls with attackers posing as colleagues, IT support, or executives. These attacks leverage deepfake technology to clone voices and even video appearances of known authority figures.

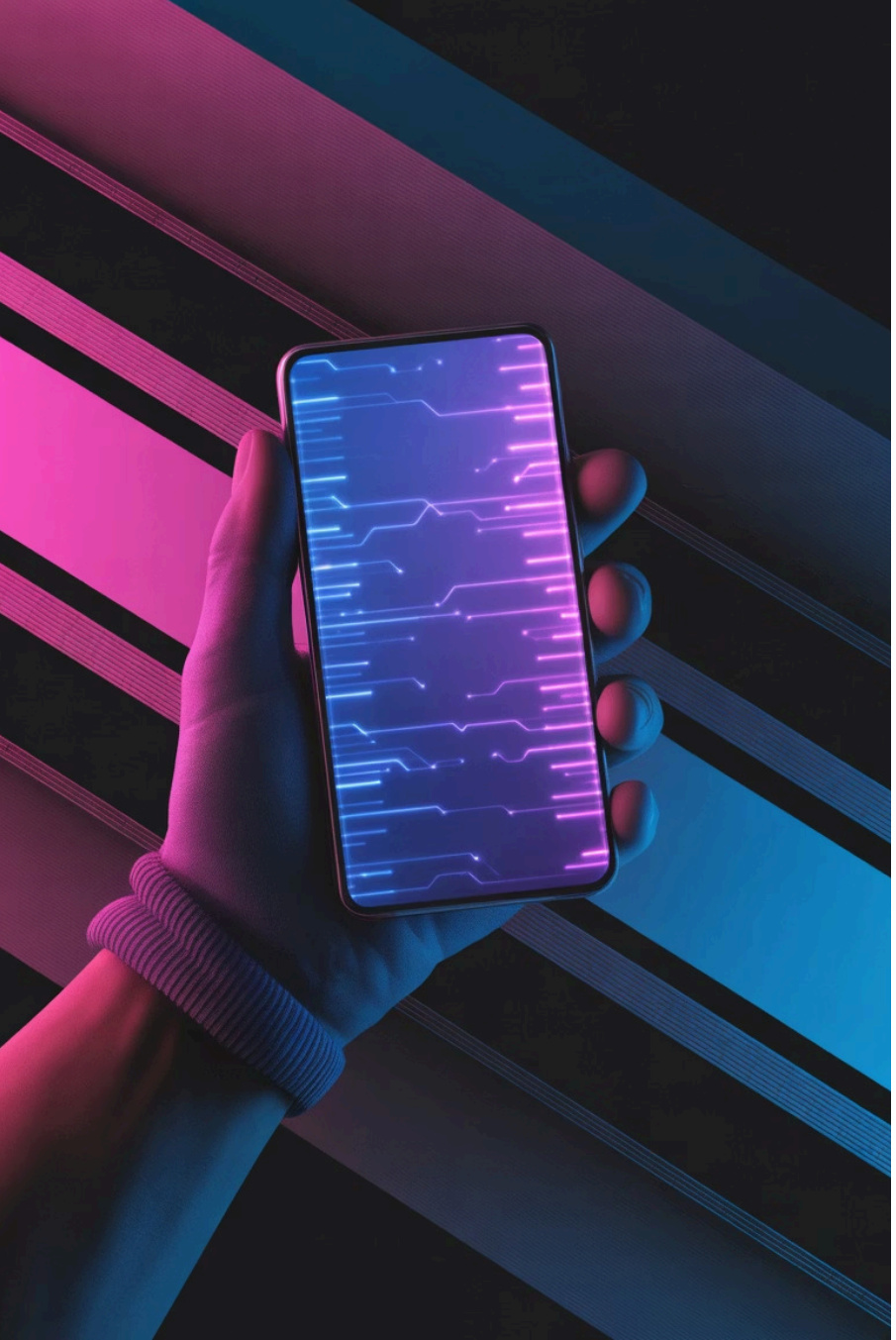
2 Persistent Engagement

Multi-day or multi-week campaigns that establish trust before executing the actual attack. These "slow burn" attacks are particularly effective against high-value targets who may be security-conscious.

3 Cross-Platform Coordination

Attacks that coordinate across multiple channels (SMS, email, phone, social media) to create a consistent illusion of legitimacy. The multi-channel approach significantly increases perceived authenticity.

These high-effort, high-touch attacks target specific high-value individuals and can result in privilege escalation in minutes once trust is established. Over one-third of successful social engineering incidents now involve non-phishing tactics that bypass traditional security awareness training.



Chapter 5

Defending Against Android Attacks

Effective Android security requires a multilayered approach that addresses technical vulnerabilities while also strengthening the human elements of security. Modern defence strategies must be comprehensive, adaptive, and continuously evolving.

The following strategies represent best practices for protecting Android devices and users from the complex threat landscape of 2025, combining technical controls with human-focused security measures.

Strategies for Protection

Advanced Mobile Threat Defence

- Deploy AI-powered behavioural analytics to detect anomalous app and network activity
- Implement on-device phishing protection with real-time URL scanning
- Establish continuous vulnerability assessment for installed applications

Zero Trust Implementation

- Apply conditional access based on device posture, location, and risk signals
- Implement identity threat detection to identify compromised credentials
- Enforce least-privilege access controls for all mobile applications

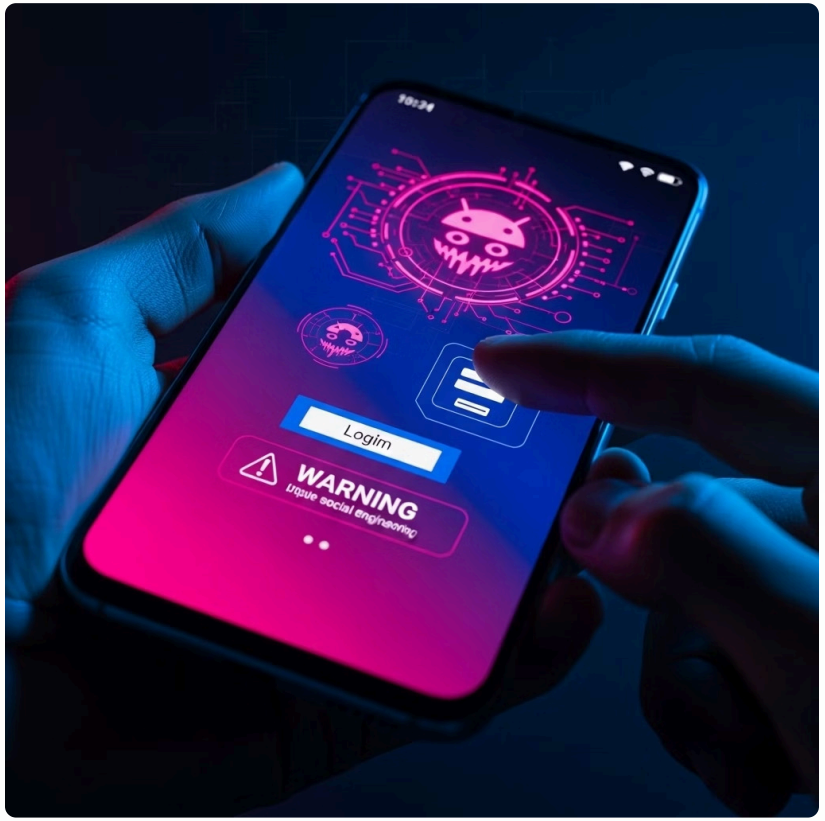
Application Security Controls

- Restrict sideloading through technical controls and compliance policies
- Deploy app vetting tools to assess security of work-related applications
- Monitor app communications for data sovereignty and privacy concerns

Human-Centric Security

- Deliver contextual, just-in-time training based on actual user behaviour
- Implement secure communication channels for verifying suspicious requests
- Create psychological safety for reporting potential security incidents

Conclusion: The Human Factor is the Frontline



Android attacks in 2025 exploit both technology and human psychology at unprecedented scale. As technical defences improve, attackers increasingly target the human element through sophisticated social engineering.

Organisations must prioritise mobile security as business-critical, combining:

- Advanced technical controls
- Human-centric security awareness
- Comprehensive security policies
- Continuous monitoring and adaptation

> The strongest firewall is an informed and alert user who recognises manipulation attempts and follows security best practices.