Executive Incident Report

Case ID: 2025-09-10-001
Prepared by: Oluwaniyi Damilare Enoch

Date & Time: 2025-09-10, 11:00 – 13:00

Severity Level: Medium

Category: Phishing

Executive Summary

A suspicious URL (hxxps[://]sites[.]google[.]com/view/xksl/home) was identified and investigated. The site impersonated GMX, a popular brand (email provider and crypto exchange). Multiple URL reputation checks confirmed the site and its redirects as malicious (phishing).

The phishing chain redirected through a Google link to a Netlify page (`wonderful-ganache-327ff8.netlify.app`), which has since been taken offline. The intended purpose was likely credential harvesting.

Incident Details

Investigation Findings

- Initial URL: hxxps[://]sites[.]google[.]com/view/xksl/home
- Observed Behavior: Displayed GMX phishing page with "Click Here" button.
- Redirect Chain:
    - Google Sites → Google Redirect → Netlify hosted page
- Final Destination: Netlify site (offline at time of investigation).
- Reputation: All three URLs flagged as phishing on VirusTotal.
- MITRE ATT&CK Mapping: T1566.002 (Phishing via link)

Impact Assessment

- No active malware payload was observed.
- If live, users who clicked through may have exposed login credentials**.**
- Business risk: Compromise of email accounts could enable further phishing, business email compromise, or data leakage.
- Severity justification: Rated Medium due to limited exposure (site offline during analysis, no payload detected), though credential theft was the likely objective.

Recommendations

1. Block the identified URLs at the network level.
2. Alert users to be cautious of GMX-themed phishing attempts.
3. Monitor logs for any connections to the flagged Netlify domain and similar credential-harvesting campaigns.
4. Submit takedown requests for phishing pages if still active.

Conclusion

This was a confirmed phishing attempt leveraging Google Sites and Netlify as hosting platforms. The primary goal was likely credential theft targeting GMX users. Although the page is offline, the infrastructure indicates an active phishing campaign. Similar attempts may reappear, and proactive monitoring is recommended**.**