Phishing Email Analysis Report

Analyst: Alexander T. Ramos
Date: October 05, 2025

Executive Summary

A suspicious email was reported by a user claiming to be from “SecureHelpDesk.” Upon analysis, the email was determined to be a phishing attempt designed to harvest user credentials through a fake password reset link. The link directed users to **https://securehelpdesk.info/login/update-password**, a domain not associated with the legitimate company. Investigation of the email headers revealed discrepancies between the sender domain and the reply-to address.

Technical Analysis

- Sender Domain: securehelpdesk.info
- Legitimate Domain: securehelpdesk.com
- Observed Issue: Domain spoofing (typosquatting)
- Malicious Link: https://securehelpdesk.info/login/update-password
- IP Address (Resolved): 156.248.192.23
- Hosting Provider: Contabo GmbH (Germany)
- Malware Detection: VirusTotal flagged 4/68 engines for phishing

Indicators of Compromise (IOCs)

Type	Indicator	Description
Domain	securehelpdesk.info	Typosquat phishing domain
URL	https://securehelpdesk.info/login/update-password	Credential harvesting page
IP	156.248.192.23	Hosting server
File Hash	—	No attachment present

Recommendations

1. Block the domain securehelpdesk.info and IP 156.248.192.23 on all endpoints and firewalls.
2. Notify users not to click the link or enter credentials.
3. Update spam filters and implement DKIM/DMARC enforcement.
4. Conduct user awareness training on identifying phishing red flags.

Conclusion

The phishing attempt demonstrates the importance of validating sender domains and using multi-layered email security. Future prevention efforts should focus on strengthening security awareness and improving automated email filtering systems.

Appendix

See email_investigation.md for full header and body analysis, and IOCs.csv for structured threat data.