Incident Report – Phishing Email Analysis

1. Executive Summary

On 7 September 2022, a suspicious email was detected claiming to originate from MetaMask Support. The message urged recipients to verify their wallets within five days to avoid termination. Upon detailed analysis, the email was confirmed to be a phishing attempt leveraging both a malicious URL and a QR code (Quishing). Immediate containment actions were taken to block the threat.

2. Email Details

Date/Time: 07 September 2022 – 21:36:59 (+0200)
Subject: Security Alert
From: metamask-updates-action@netwrksecurity.com
To: phishing@pot
Sender IP: 94.231.103.45
Resolved Host: websmtp-out1.simply.com
Message ID:

3. Technical Analysis - Sender Verification

- Originating IP belongs to websmtp-out1.simply.com (legitimate service).
- Email headers failed SPF, DKIM, and DMARC authentication → strong indication of spoofing.
- Domain netwrksecurity.com resembles networksecurity.com, pointing to typosquatting. The domain is parked and potentially exploitable by malicious actors.

3. Technical Analysis - Content Review

- Message impersonates MetaMask Support.
- Claims that non-verified wallets will be disabled by 12 September 2022.
- Provides both a “verification” hyperlink and a QR code to trick victims into revealing credentials.

3. Technical Analysis - URL Analysis

- Extracted link: hxxps[://]420[.]bio/NtRIA
- Classified as malicious by multiple security vendors (linked to phishing/malware).

3. Technical Analysis - Attachment Analysis

- No attachments were present.

4. Risk Assessment

- Phishing / Credential Theft: High probability due to impersonation of a known crypto wallet provider.
- Quishing (QR Phishing): Increases risk by targeting mobile device users.
- Brand Damage: Potential erosion of trust in MetaMask brand.

- User Impact: Possible compromise of crypto wallet credentials and financial loss.

Overall Risk Level: HIGH

5. Mitigation & Defense Actions

- Blocked sender IP (94.231.103.45) at the network perimeter.
- Blacklisted malicious domain and URL (420[.]bio/NtRIA) to prevent user access.
- Reported the phishing campaign to relevant security channels for broader awareness.
- Recommended organization-wide security awareness training on QR code–based phishing.

6. Conclusion

This phishing attempt demonstrates the use of spoofed domains, malicious links, and QR codes to bypass user suspicion. The proactive blocking of the IP and URL minimized exposure. Continuous monitoring and user training are essential to mitigate similar threats in the future.