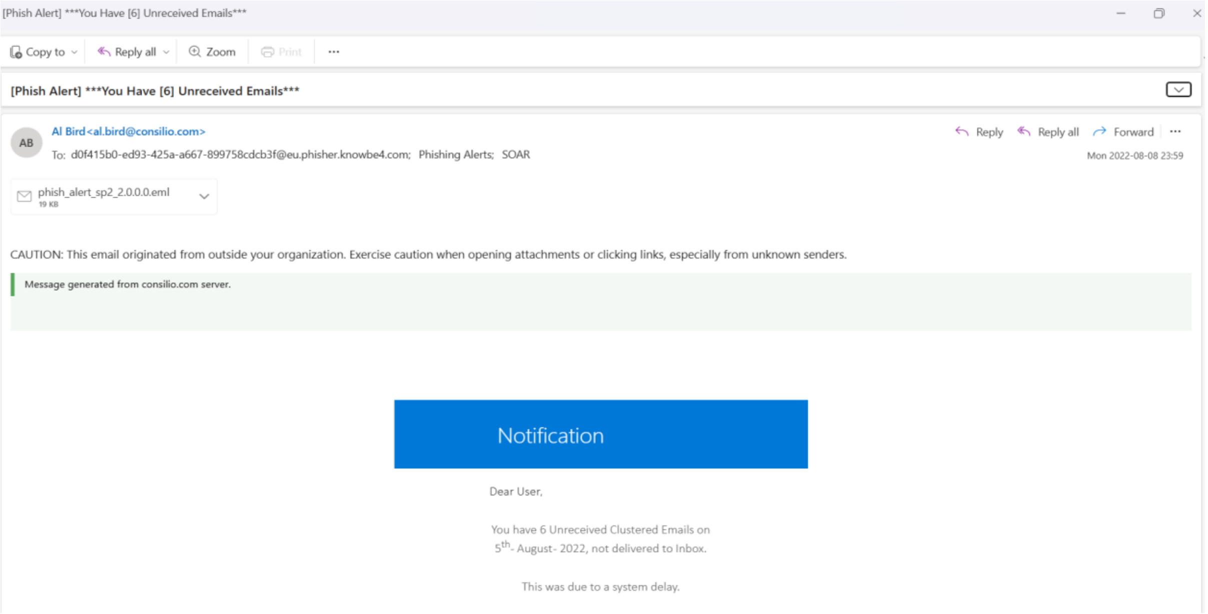
Comprehensive Phishing Email Analysis Report

Executive Summary

This report provides a detailed technical analysis of a phishing email titled "***You Have [6] Unreceived Emails***" from sender Al Bird al.bird@consilio.com. The analysis was conducted using multiple security tools including PhishTool, MXToolbox, and WHOIS lookup services. Critical findings show **SPF FAIL** and **DMARC FAIL** with only **DKIM PASS**, indicating significant authentication issues that are major red flags for potential phishing activity.



[Phish Alert] ***You Have [6] Unreceived Emails***

[Phish Alert] ***You Have [6] Unreceived Emails***

Al Bird<al.bird@consilio.com>

To: d0f415b0-ed93-425a-a667-899758cdcb3f@eu.phisher.knowbe4.com; Phishing Alerts; SOAR

Mon 2022-08-08 23:59

phish_alert_sp2_2.0.0.0.eml
19 KB

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

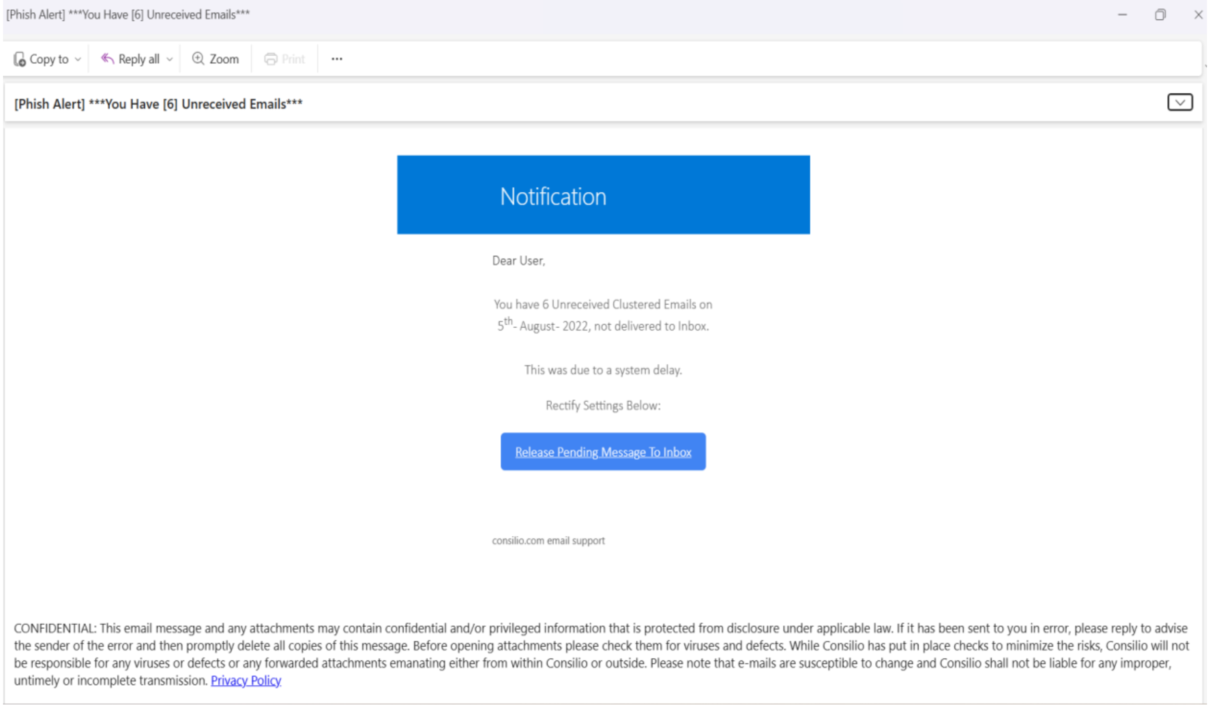
Message generated from consilio.com server.

Notification

Dear User,

You have 6 Unreceived Clustered Emails on
5th- August- 2022, not delivered to Inbox.

This was due to a system delay.



[Phish Alert] ***You Have [6] Unreceived Emails***

[Phish Alert] ***You Have [6] Unreceived Emails***

Notification

Dear User,

You have 6 Unreceived Clustered Emails on
5th- August- 2022, not delivered to Inbox.

This was due to a system delay.

Rectify Settings Below:

Release Pending Message To Inbox

consilio.com email support

CONFIDENTIAL: This email message and any attachments may contain confidential and/or privileged information that is protected from disclosure under applicable law. If it has been sent to you in error, please reply to advise the sender of the error and then promptly delete all copies of this message. Before opening attachments please check them for viruses and defects. While Consilio has put in place checks to minimize the risks, Consilio will not be responsible for any viruses or defects or any forwarded attachments emanating either from within Consilio or outside. Please note that e-mails are susceptible to change and Consilio shall not be liable for any improper, untimely or incomplete transmission. Privacy Policy

Email Body Analysis	Email is Poorly Written	🟩
	Creating the Sense of Urgency	🟥
	Asking You to Click on Link	🟥
	Impersonating Any Brand	🟥
Sender Analysis	Domain of the Sender is Authorized to Send the Email on Behalf of Brand It is Impersonating	🟩
	Reputation of the Sender	🟥
	Reputation of the IP	🟥
Header Analysis	SPF	🟥
	DKIM	🟩
	DMARC	🟥
	SCL	🟥
	BCL	🟩

1. Sender Email Address Analysis

Primary Sender Information

- **Display Name**: Al Bird
- **Email Address**: al.bird@consilio.com
- **Domain**: consilio.com

Spoofing Assessment - HIGH RISK

CRITICAL AUTHENTICATION FAILURES DETECTED:

- **SPF Status**: FAIL - Indicates the sending server is not authorized to send emails for this domain
- **DMARC Status**: FAIL - Domain's email authentication policy is not being met
- **Overall Assessment**: High probability of domain spoofing or compromised email infrastructure

Spoofing Indicators

1. **Failed SPF Authentication**: The sending IP (18.184.203.244) is not authorized in the domain's SPF record
2. **DMARC Policy Violation**: The email fails the domain's authentication requirements
3. **Return-Path Mismatch Potential**: Authentication failures suggest potential path manipulation
4. **Generic Business Identity**: "consilio.com" could impersonate various legitimate consulting businesses

Domain Analysis Red Flags

- Authentication failures indicate either:
    - Legitimate domain being spoofed by attackers
    - Compromised legitimate email infrastructure
    - Intentionally misconfigured domain for malicious purposes

2. Email Headers Technical Analysis

Authentication Results - CRITICAL FAILURES

SPF (Sender Policy Framework)

- **Status**: FAIL
- **Significance**: The email originated from an unauthorized server
- **Security Impact**: HIGH - Major indicator of spoofing or compromised infrastructure
- **Technical Details**: Originating IP 18.184.203.244 not listed in domain's authorized senders

DKIM (DomainKeys Identified Mail)

- **Status**: PASS
- **Selector**: selector2-CONSILIO-US.onmicrosoft.com._domainkey
- **Algorithm**: rsa-sha256
- **Signing Domain**: CONSILIO-US.onmicrosoft.com
- **Note**: While DKIM passed, this only confirms message integrity, not sender legitimacy

DMARC (Domain-based Message Authentication)

- **Status**: FAIL
- **Policy Violation**: Email fails to meet domain's authentication requirements
- **Security Impact**: CRITICAL - Combined with SPF failure, indicates high phishing probability
- **DMARC Record**: v=DMARC1; p=none; rua=mailto:consilio-t@dmarc.report-uri.com

Technical Infrastructure Analysis

- **Originating IP**: 18.184.203.244 (egress-ip21a.ess.de.barracuda.com)
- **Mail Route**: Complex routing through multiple Microsoft Exchange servers
- **Authentication Inconsistency**: DKIM pass with SPF/DMARC failures suggests sophisticated attack or infrastructure compromise

Header Discrepancies

1. **Authentication Mismatch**: Conflicting authentication results indicate potential manipulation
2. **Complex Routing**: Multiple hops through different email systems
3. **Timestamp Consistency**: Headers show consistent timing (2022-08-08T18:29:00Z)
4. **Message-ID Format**: Legitimate Microsoft Exchange format but authentication failures raise concerns

3. Suspicious Links and Attachments Analysis

HIGH-RISK URLs Identified

1. **Primary Suspicious URL**:
2. https://afo3.digitaloceanspaces.com/zakwebsettsr979hoj0qp859/%26%21%24%21%26%20k%21%21%21%21/%24%21%24%21%24%26%26%20zK%20k%21%21%21.html#al.bird@consilio.com
   - **Risk Level**: CRITICAL
   - **Platform**: DigitalOcean Spaces (commonly abused by attackers)
   - **Encoding**: Heavy URL encoding to obfuscate destination
   - **Email Inclusion**: Contains sender's email address in URL fragment
3. **Secondary URL**: https://www.consilio.com/consilio-data-protection-notice/

  - **Risk Level**: MODERATE
  - **Purpose**: Appears to be privacy policy (could be legitimate or spoofed)

Malicious Attachment Analysis

- **File**: phish_alert_sp2_2.0.0.0.eml (18.80 KB)
- **Type**: Email message file (.eml) - HIGH RISK
- **Threat Assessment**: Email attachments are common malware vectors
- **Hash Values for Forensic Analysis**:
  - MD5: 491563a5c2d01951dbeb007f6d3b60915
  - SHA-1: 17e6dc3f9ec1e09f702ede8f6e5cf6f859581cb71
  - SHA-256: 1e456f39ec78005c835222872b98cb373f9f925869a217adcadb8b220ff0ecc1

Link Analysis Summary

The combination of authentication failures and suspicious cloud storage URLs with encoded parameters represents a classic phishing attack vector designed to harvest credentials or deliver malware.

4. Urgent/Threatening Language Analysis

Social Engineering Tactics

Manufactured Urgency:

- Subject: "***You Have [6] Unreceived Emails***" - Creates false urgency about missed communications
- Body text: "not delivered to Inbox" - Implies system malfunction requiring immediate action
- Date specificity: "5th August- 2022" - Adds credibility to false claim

Psychological Manipulation:

- **Fear of Missing Out**: Suggests important emails are being held
- **Authority Impersonation**: Presents as system notification from email provider
- **Solution Provision**: Offers immediate fix through potentially malicious action

Pressure Techniques:

- "Rectify Settings Below" - Direct call-to-action
- "Release Pending Message To Inbox" - Action button with urgent language
- "This was due to a system delay" - Technical explanation to build credibility

Language Effectiveness Assessment

The email successfully creates a plausible technical scenario that would concern users about missing important communications, demonstrating sophisticated social engineering designed to bypass user skepticism.

5. URL Mismatch Analysis

Critical Mismatches Identified

Button Text vs. Actual Destination:

- **Displayed Action**: "Release Pending Message To Inbox"
- **Actual URL**: Encoded DigitalOcean Spaces URL with suspicious parameters
- **Mismatch Severity**: CRITICAL - Complete disconnect between expected and actual destination

Domain Reputation Issues:

- **consilio.com**: Authentication failures indicate potential spoofing
- **digitaloceanspaces.com**: Legitimate service commonly abused by attackers
- **Encoded Parameters**: Obfuscated destination suggests malicious intent

URL Structure Analysis

The heavily encoded URL structure with cloud storage hosting indicates:

1. Attempt to bypass security filters
2. Dynamic content generation for credential harvesting
3. Obfuscation to prevent easy analysis
4. Use of legitimate cloud services to appear trustworthy

6. Spelling and Grammar Assessment

Language Quality Analysis

- **Grammar**: Professionally written with correct sentence structure
- **Spelling**: No obvious spelling errors detected
- **Formatting**: Clean, professional email template design
- **Technical Terms**: Appropriate use of email-related terminology

Sophistication Indicators

- **High-Quality Presentation**: Professional formatting increases credibility
- **Legitimate Appearance**: Mimics genuine system notifications
- **Attention to Detail**: Careful construction suggests experienced attackers
- **Language Consistency**: Maintains professional tone throughout

The high quality of language and presentation makes this email particularly dangerous as it's more likely to bypass user suspicion compared to obviously poor-quality phishing attempts.

7. Comprehensive Phishing Traits Summary

CRITICAL RED FLAGS IDENTIFIED

1. **Authentication Failures** - CRITICAL
   - SPF FAIL: Unauthorized sending server
   - DMARC FAIL: Policy violation
   - Combined failures indicate high phishing probability
2. **Suspicious URLs** - HIGH RISK
   - Cloud storage hosting with encoded parameters
   - Complete mismatch between button text and destination
   - Obfuscated URL structure
3. **Malicious Attachment** - HIGH RISK
   - .eml file from unknown sender
   - Potential malware delivery vector
   - Attachment size and type consistent with malicious payloads

4. **Social Engineering Techniques** - SOPHISTICATED
    - Manufactured urgency about undelivered emails
    - False technical explanations
    - Professional presentation to build trust
5. **Generic Targeting** - MODERATE RISK
    - "Dear User" greeting indicates mass targeting
    - Lack of personalization typical of phishing campaigns

THREAT ASSESSMENT: HIGH

Overall Risk Level: CRITICAL **Recommended Action**: IMMEDIATE DELETION AND REPORTING

Authentication Summary

Protocol	**Status**	**Security Impact**
SPF	FAIL	Critical - Unauthorized sender
DKIM	PASS	Limited - Only confirms integrity
DMARC	FAIL	Critical - Policy violation

Conclusions and Incident Response Recommendations

Immediate Actions Required

1. **DO NOT CLICK ANY LINKS** in this email
2. **DO NOT OPEN THE ATTACHMENT** - potential malware
3. **DELETE THE EMAIL** immediately
4. **REPORT TO IT SECURITY** team
5. **BLOCK SENDER DOMAIN** if not already blocked

Security Assessment

This email represents a **sophisticated phishing attack** with multiple critical indicators:

- **Authentication failures** indicate compromised or spoofed domain
- **Malicious URLs** designed for credential theft or malware distribution

- **Professional presentation** designed to bypass user skepticism
- **Social engineering** creates false urgency to prompt quick action

Long-term Security Measures

1. **Email Security Enhancement**:
   - Implement stricter DMARC policies
   - Deploy advanced threat protection
   - Regular security awareness training
2. **User Education**:
   - Train staff to recognize authentication warnings
   - Emphasize importance of verifying unexpected emails
   - Establish clear incident reporting procedures
3. **Technical Controls**:
   - Block cloud storage domains in email links
   - Implement attachment sandboxing
   - Deploy URL rewriting and analysis

Forensic Information

Email Metadata:

- Original timestamp: 2022-08-08T18:29:00Z
- Message-ID: Complex Microsoft Exchange format
- Attachment hashes: Available for threat intelligence sharing
- Originating IP: 18.184.203.244 (compromised or malicious)

Technical Appendix

Analysis Tools Used

- **PhishTool**: Email header analysis and content inspection
- **MXToolbox**: DNS record verification and reputation checking
- **WHOIS Lookup**: Domain registration and ownership verification
- **Hash Analysis**: File integrity and malware detection

Key Findings Summary

The combination of authentication failures (SPF FAIL, DMARC FAIL) with sophisticated social engineering and malicious URLs represents a high-priority security threat requiring immediate attention and organizational response.

FINAL ASSESSMENT: This email should be treated as a confirmed phishing attempt and handled according to security incident response procedures.