Theotismatthews
From: teamsupport-904714550350403@questionprov101621.com
To: support_5368058@googlemail.com

Wed, Dec 17 at 9:08 AM

For your security we disabled all images and links in this email. If you believe it is safe to use, mark this message as not spam.
Show images

Unusual activity detected on your inbox

Our automated email protection system detected suspicious behavior associated with your inbox.

Immediate review is required to maintain full email functionality.

Threat Type: Suspicious Login Pattern
Detected Location: Unknown Network
Time Detected: Today
Protection Status: Partially Limited

RISK LEVEL: HIGH

Plus member number and user name is LMGNNTJAJKAVDDONMJOISOBQW Your membership delivers faster reservations and rentals, a special members-only line at major airport locations and exclusive discounts In addition, you'll be able to start earning points you can redeem for Free Rental Days after you activate your rewards Please allow 24 hours for system updates before activating To get the most from your next rental, simply go to http and log in with your member number Thank you for choosing Enterprise We look forward to making your next rental experience more rewarding Hi TDUDLOPXVCLPMMYWMT, My name's Dylan Basile and I work at Event Temple Nice to meet you and thanks for requesting a demo Joining me for a quick demo will be the fastest and most efficient way for you to see what the software is capable of Did any of the times on our website work for you and if so, were you able to schedule a demo okay? Here they are again calendly com dylan-eventtemple 30min If not, just let me know and we'll find something else -- Dylan Basile *Book a demo with me here * Hi AQINDSBLKPMBMGEGJQVYOQBZF, Thanks for signing up, and congratulations on your new mis nlejyxkogxrzydkopl account! You'll find everything you need to get started below, and if you need additional help there's a link to our support forum at the bottom === Account Information === Username AVQHFGCEVSFUYTGCDFANUHLMG Site ID JPQYFBYBSFGZIKUBQPZKWCNBC === Your Account Console === Thanks again! Team misbvjmiqwxguditeazka Powered by mishvuimjiwgkkhnldxxl < title> Dear NTJTOMBHQCGBCOXXXKHFHNQRU EDYBAJOUTIIFKQWNXYPLVNIGU, Welcome to the Enterprise Plus? membership experience Your Enterprise Plus member number and user name is ONHFECJHAKIKZDEIMKTCGGZFW Your membership delivers faster reservations and rentals, a special members-only line at major airport locations and exclusive discounts In addition, you'll be able to start earning points you can redeem for Free Rental Days after you activate your rewards Please allow 24 hours for system updates before activating To get the most from your next rental, simply go to http and log in with your member number Thank you for choosing Enterprise We look forward to making your next rental experience more rewarding == You need a budget, and your email needs confirmation == Hello! Quick note to let you know that your email needs to be confirmed before all sorts of great things happen Like your being able to use YNAB all along your road to budgeting glory Please confirm by clicking the link below Confirm your email Thank you! And we're serious about budgeting glory It's a real thing, and you will bask in it Regards, The YNAB Team < Dear Dalewoowood mislajuhdiukoynxgoioy, Welcome to the Enterprise Plus? membership experience Your Enterprise Plus member number and user name is ISCQENJGTQGYMSZVM Your membership delivers faster reservations and rentals, a special members-only line at major airport locations and exclusive discounts In addition, you'll be able to start earning points you can redeem for Free Rental Days after you activate your rewards Please allow 24 hours for system updates before activating To get the most from your next rental, simply go to http and log in with your member number Thank you for choosing Enterprise

1. Executive Summary

Ticket ID: PH-2025-001
Date/Time Detected: 17-Dec-2025, 9:08 AM
Reported By: User Inbox / SOC Monitoring
Threat Type: Phishing Email
Severity: Moderate
Status: Contained / Closed

Summary / Description:

- Phishing email received in monitored user inbox.
- Indicators observed: grammatical errors, suspicious sender attributes, deceptive fine print, and false urgency.
- No user interaction; no compromise detected.

Actions Taken:

- Blocked malicious domain and source IP address.
- Monitored for further activity; no additional incidents observed.

Impact Assessment:

- Moderate risk: potential for credential compromise or malware delivery if interacted with.
- Immediate mitigation successfully reduced exposure.

Recommendations:

- Continue user awareness and training on phishing threats.
- Maintain proactive email filtering and security controls.
- Consider periodic simulated phishing campaigns to test detection and response.

2. Objective & Scope

- Purpose of the report
    - The purpose of this phishing report is to analyze and highlight multiple red flags present in the examined email, such as poor grammar, anomalous

sender behavior, and social engineering tactics designed to create a false sense of urgency.

3. Incident Overview / Attack Summary

- Date & time: 12/17/2025 9:08 AM
- This phishing attempt was identified through the analysis of multiple indicators, including anomalous email characteristics, grammatical inconsistencies, artificially induced urgency, and deceptive fine print commonly used in social engineering attacks.

4. Attack Vector & Methodology

Include:

- teamsupport-904714550350403@questionprov101621.com , support_5368058@googlemail.com
- Subject line analysis: Theotismatthews, Action Required: Email Activity Reported

5. Impact Assessment

- Number of users who interacted: 1
- Credentials exposed?: No
- Potential access gained: No
- Business risk level: Moderate
    - Low / Medium / High / Critical

Had the phishing email been interacted with, the user could have been redirected to a malicious domain designed to harvest authentication credentials or deliver malicious payloads. Successful exploitation may have resulted in account compromise, unauthorized access to internal systems, and potential escalation of privileges. Additionally, malware execution could have enabled persistence, lateral movement, data exfiltration, or ransomware deployment. Such activity would significantly increase

organizational risk, potentially impacting system integrity, data confidentiality, and business operations.

6. Detection & Response Actions

- How the phishing was detected: The phishing attempt was identified after the email was received in a monitored user inbox and subsequently reviewed for suspicious indicators.
- Security tools involved:
  - Email gateway
- Actions taken:
  - Link blocking
  - Password resets
  - User notifications
  - Account monitoring

7. Mitigation & Remediation

Short-Term

- As a short-term mitigation measure, the associated malicious domain and source IP address were blocked to prevent further interaction and potential exploitation.

Long-Term

- Phishing awareness training
- Email security hardening

8. Conclusion

- Overall, this phishing attempt posed a **moderate risk** to the organization. While no user interaction occurred, the email demonstrated multiple social engineering

indicators capable of leading to credential compromise or malware delivery if acted upon. Timely identification and containment actions, including domain and IP blocking, effectively reduced the likelihood of further exposure