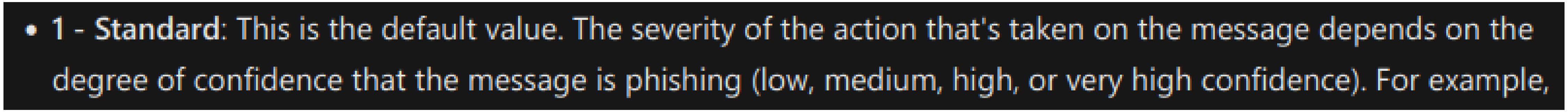
Changing anti-phishing threshold protection for the IT dept for testing

Roman Sumailov

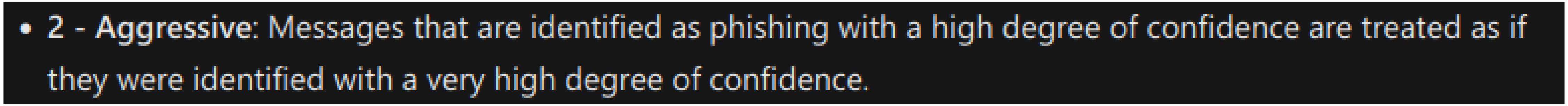
ASDF 17.10.2024

Changing phishing threshold for Exchange Online

- **From 1 (default) to 2 (aggressive)**



- **1 - Standard**: This is the default value. The severity of the action that's taken on the message depends on the degree of confidence that the message is phishing (low, medium, high, or very high confidence). For example,



- **2 - Aggressive**: Messages that are identified as phishing with a high degree of confidence are treated as if they were identified with a very high degree of confidence.

- **Recommendation of the 2023 Cyber-Security Audit (R-21.6)**
- **In total 4 levels:**
  1. **Standard**
  2. **Aggressive**
  3. **More aggressive**
  4. **Most aggressive**

Impact: Probably none

MS internal phishing levels according to threshold docs	Distinguishable phishing levels in MS Defender and email headers
1. Low 2. Medium 3. High 4. Very high	1. Normal 2. High - We quarantine these emails

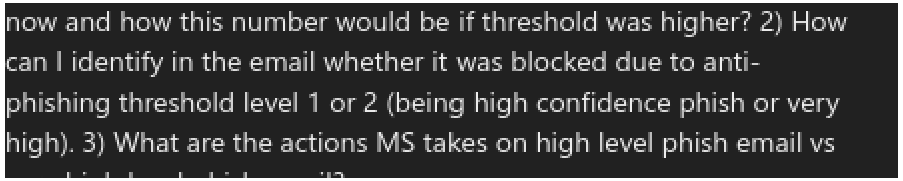
- **Currently - high-level confidence (right column) phishing emails are quarantined**
- **Change will make the system treat high-level confidence phishing emails as if they were very high confidence level (left column)**
- **Unclear if there are additional differences for “very high confidence phishing” - Support ticket with Microsoft open for clarification**
- **Probably high level phish emails will continue being quarantined as they do now**
- **Probably it will not increase emails quarantine rate**

Please report to the Computer Security Team increased false positives rate

Docs link - https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about#advanced-phishing-thresholds-in-anti-phishing-policies-in-microsoft-defender-for-office-365

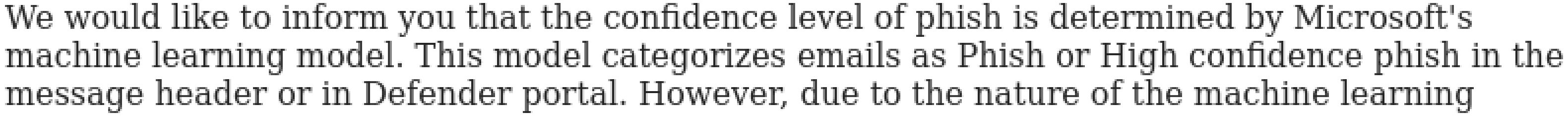
MS support on Anti-phishing threshold levels

Roman



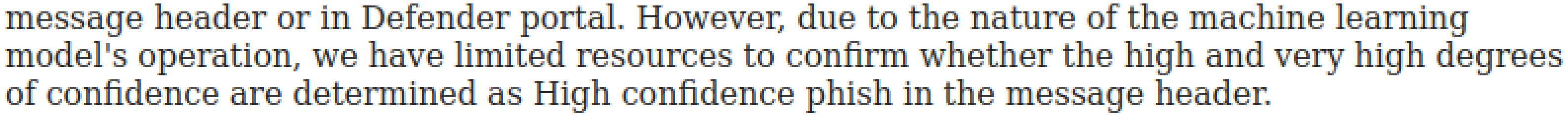
now and how this number would be if threshold was higher? 2) How can I identify in the email whether it was blocked due to anti-phishing threshold level 1 or 2 (being high confidence phish or very high). 3) What are the actions MS takes on high level phish email vs

MS



We would like to inform you that the confidence level of phish is determined by Microsoft's machine learning model. This model categorizes emails as Phish or High confidence phish in the message header or in Defender portal. However, due to the nature of the machine learning

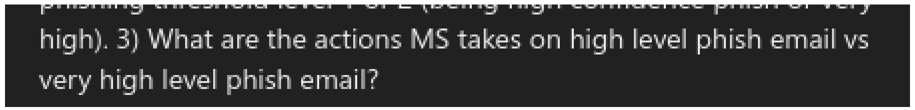
…MS



message header or in Defender portal. However, due to the nature of the machine learning model's operation, we have limited resources to confirm whether the high and very high degrees of confidence are determined as High confidence phish in the message header.

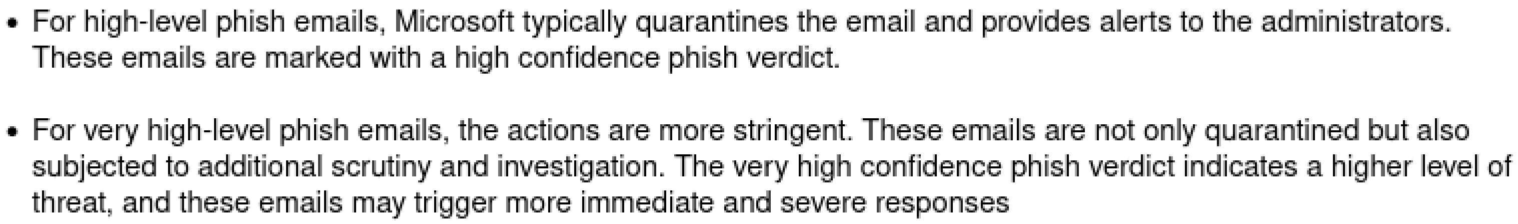
MS support on Anti-phishing threshold levels (contd.)

Roman



phishing threshold level 1 or 2 (being high confidence phish or very high). 3) What are the actions MS takes on high level phish email vs very high level phish email?

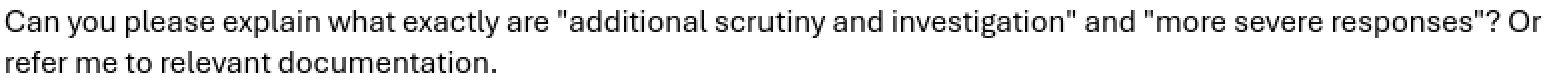
MS



- For high-level phish emails, Microsoft typically quarantines the email and provides alerts to the administrators. These emails are marked with a high confidence phish verdict.

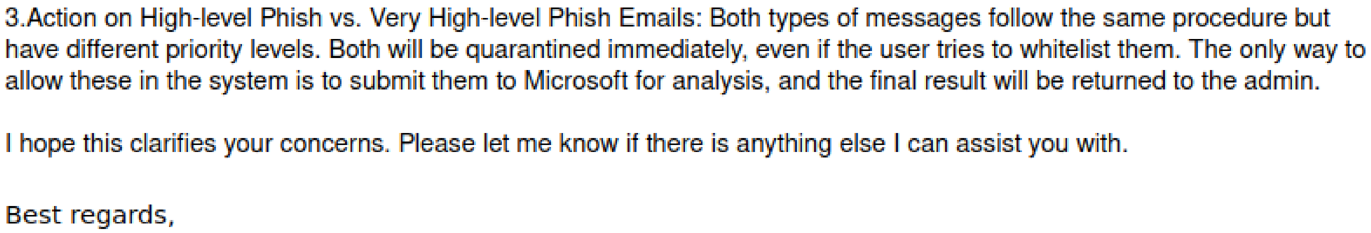
- For very high-level phish emails, the actions are more stringent. These emails are not only quarantined but also subjected to additional scrutiny and investigation. The very high confidence phish verdict indicates a higher level of threat, and these emails may trigger more immediate and severe responses

Roman



Can you please explain what exactly are "additional scrutiny and investigation" and "more severe responses"? Or refer me to relevant documentation.

MS



3.Action on High-level Phish vs. Very High-level Phish Emails: Both types of messages follow the same procedure but have different priority levels. Both will be quarantined immediately, even if the user tries to whitelist them. The only way to allow these in the system is to submit them to Microsoft for analysis, and the final result will be returned to the admin.

I hope this clarifies your concerns. Please let me know if there is anything else I can assist you with.

Best regards,

Enabling impersonation protection for the IT dept for testing

Roman Sumailov

ASDF 17.10.2024

Enabling impersonation protection

- **Recommendation of the 2023 Cyber-Security Audit (R-21.6)**
- **Microsoft feature for protecting VIP accounts from being impersonated**
- **Based on display name + email address**
- **Max 350 email addresses can be protected per organisation**

Functionality description:

1) **Malicious actor sends email with display name “Roman Sumailov” from “roman.sumailov@hotmail.com” to any of you & asks for money/nudes**
2) **This gets detected & blocked**

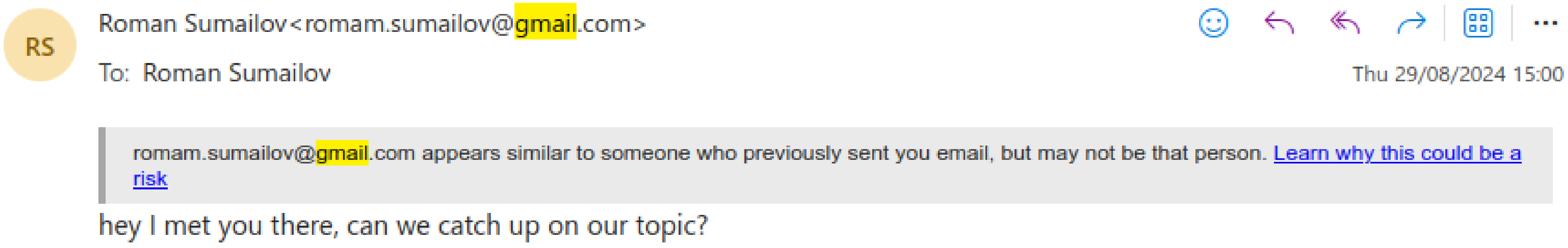
Nuances:

- **MS has safeguards to avoid blocking emails for simply similar/overlapping names**
- **Impersonated emails moved to Junk folder**

Docs link - https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about#user-impersonation-protection

Impersonation protection (2) Tips

- **First contact, impersonation & unusual character tips are enabled**



RS

Roman Sumailov<romam.sumailov@gmail.com>

To: Roman Sumailov

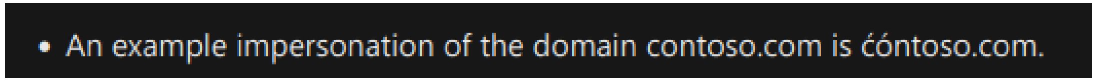
Thu 29/08/2024 15:00

romam.sumailov@gmail.com appears similar to someone who previously sent you email, but may not be that person. Learn why this could be a risk

hey I met you there, can we catch up on our topic?

Impersonation protection for domain

- Analogous workflow for domain as for users



- An example impersonation of the domain contoso.com is ćóntoso.com.

- Enabled for CERN domains: cern.ch, alumni.cern, mail.cern.ch etc

Please report to the Computer Security Team any false positives

Questions?

pls no hard questions

home.cern