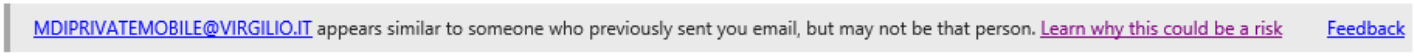
Anti-Phishing Policy - Security Banner

Overview

This tool is intended to inform users to possible scam email messages that many University students and staff receive every week.

- The policy compares an incoming email message to the history of messages in your Inbox
- When the **name** on the message matches a **name** in your email history, but the **address** is different from the previous **address**, then the anti-phishing policy flags that message as dangerous, adding a banner at the top to warn you of the anomaly



- Be careful with any email message containing a banner as above.
- If the message appears to come from your manager or co-worker, then confirm the message by calling a known number or sending a separate message to their University account. (Do not use any number or email address found within the actual email)

Benefits

Will anti-phishing policy flag a legitimate email as suspicious?

- Yes - sometimes. People often mistakenly send a legitimate email from their personal account rather than their University account.
- This happens most often when the sender is using their mobile device to send a message because the native email app is probably configured to send email for both personal and University business.

How can I prevent legitimate messages I send from being flagged with a security banner?

- The best way to prevent your messages from being flagged is to ***always*** use your University email address to send messages to colleagues and students at JU.
- Use **the Outlook Mobile** app to manage your University email and use the native email app to manage your personal email. Using separate email apps for work and personal email is the best advice.

Methods

Many of University employees are targeted each week by a simple scam that can scam you personally out of thousands of kronor or thousands of JU funds. It is very simple and thus effective. The attacker uses the University web site to find a list of employees who report to an individual like a Dean or a Manager.

The attacker creates a legitimate email address with that manager's name, such as MDIPRIVATEMOBILE@VIRGILIO.IT.
The attacker then sends a simple message:

From: Dean Deansson <MDIPRIVATEMOBILE@VIRGILIO.IT>

MDIPRIVATEMOBILE@VIRGILIO.IT appears similar to someone who previously sent you email, but may not be that person. Learn why this could be a risk Feedback

Subject: betalning

Hej

Vi behöver skicka en betalning på 17850,00 € till Belgien idag.

Det går att ordna?

vilken information behöver du för att göra denna betalning?

Med vänlig hälsning

Dean Deansson

Dean JU

The attacker can also try to convince you to purchase gift cards and send pictures of the activation codes on the gift cards. This attack is most effective against new employees.