August 2025 Phishing Scenario Results

As part of our Security Awareness Education Program, the Office of Information Technology (OIT) sent a simulated phishing scenario titled, *Your Statement is Ready for Download*. Phishing emails are specifically written to provoke an emotional response, such as **Fear, Curiosity, and Reward**. The goal is to get you to react and not think through the request or content.

This scenario used **Curiosity** as a trigger by intentionally not naming the account or business entity for the statement. The attacker knows the recipient's next logical step to glean more information on the origin of the "statement" is to click the "Download Statement" link.

The vague and generic wording in this email is your cue to **Stop, Think**, and **REPORT**. Do not fall for the trick by clicking the link in hopes of finding more information.

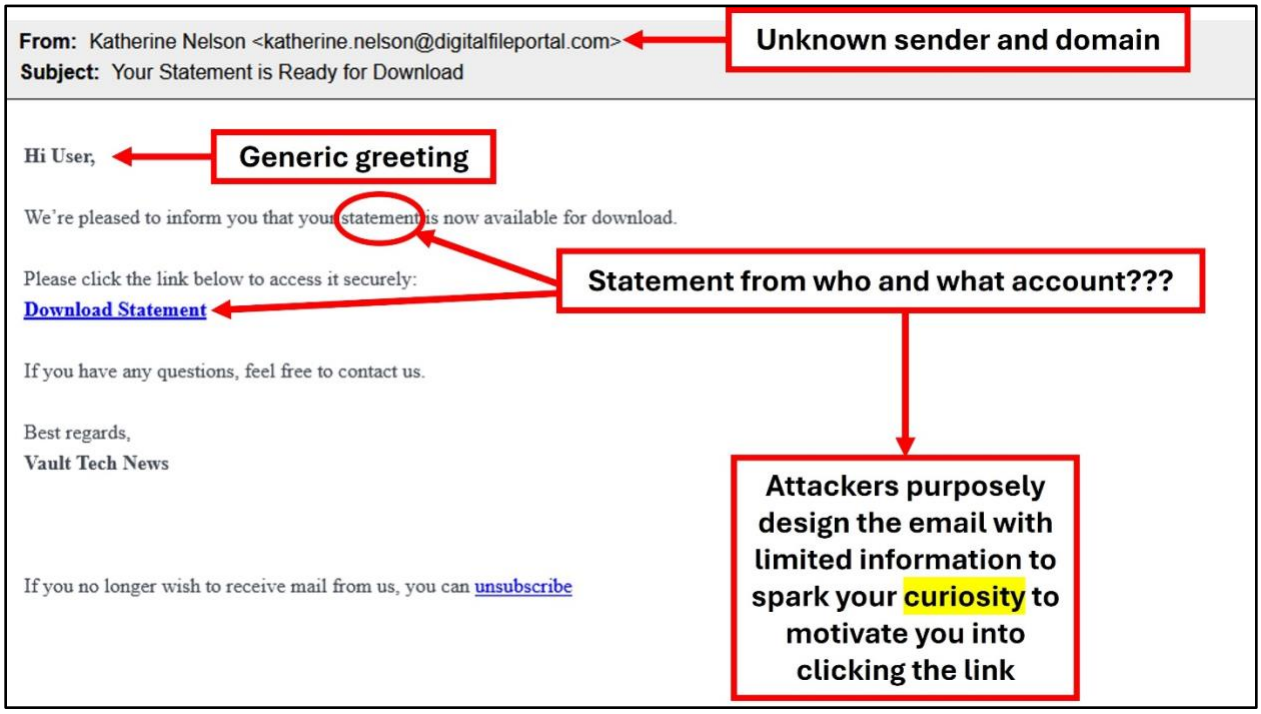
Good News

1212 employees reported the phishing scenario to the Phishtrap. Nice work MC!

Opportunities for Improvement

98 employees clicked the link within the training email. *If you were one of the clickers consider retaking Data Security training within Workday MC Learns*.

In a real-world phishing attack clicking the link may have prompted you to give up your login credentials. View the red flags in the August phishing scenario:



If you suspect an email may be a phishing attempt let IT Security analyze the email for you by REPORTING the email using the report phishing button.