February Phishing Scenario Results

OIT's February phishing simulation email was titled, *Notification!!* and mimicked messages that impersonate official government agencies. These phishing attacks attempt to trick recipients into clicking malicious links and entering login credentials on fake websites.

Understanding the warning signs helps protect both your personal and workplace accounts.

Clues to Spot in this Scenario:

Unusual Sender

- The sending email address was *care@socialsmp.com*. This is an unknown sender not associated with the Social Security Administration (SSA)
- The message was delivered to your MC email address, even though SSA related communications should go to your personal email address.

What to do: Create your personal "my Social Security" account using your PERSONAL email address only. Learn more about creating an account at https://www.ssa.gov/myaccount/

Four Basic Signs of a Scam:

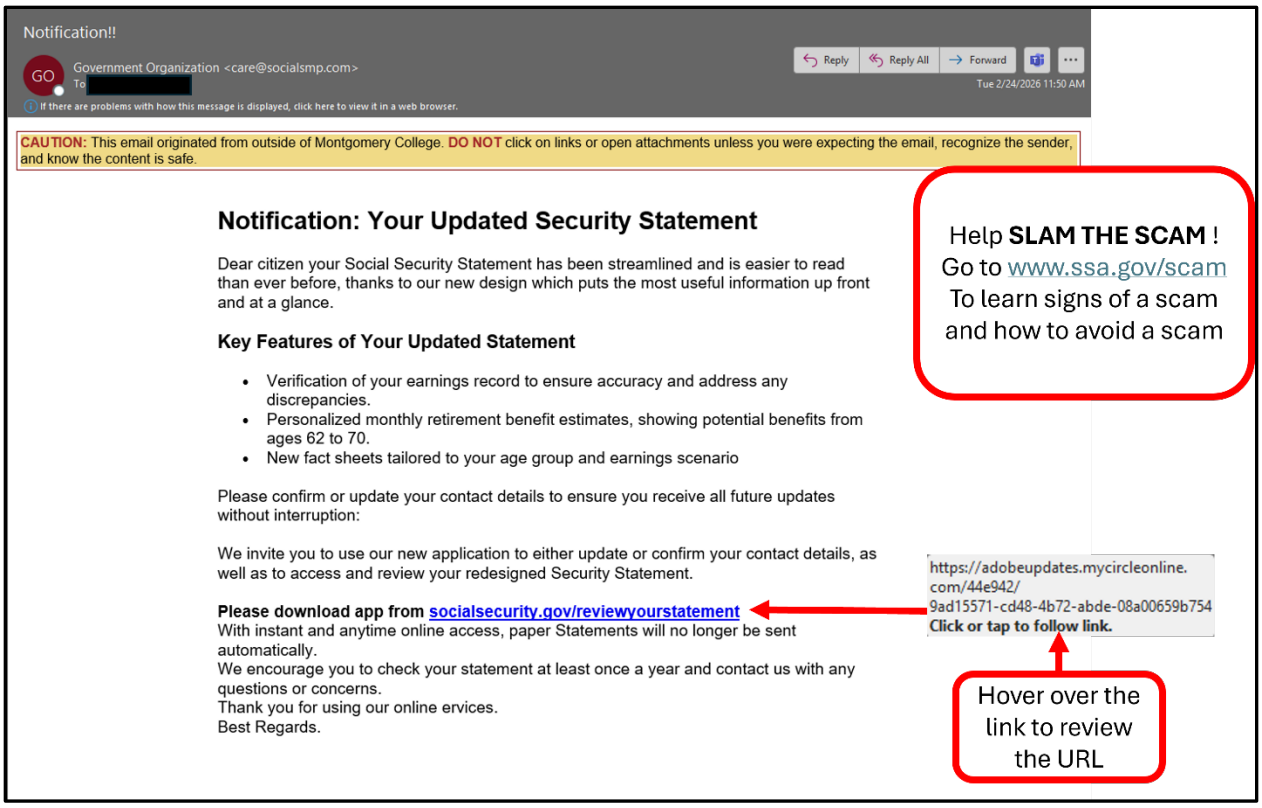
- Scammers pretend to be from an agency or organization you know to gain your trust.
- Scammers claim there is a problem or that you have won a prize.
- Scammers pressure you to act immediately.
- Scammers tell you to pay in a specific way.

What to do: The Social Security Administration (SSA) is promoting "Slam the Scam", a campaign to raise awareness of SSA-related fraud. Visit https://www.ssa.gov/scam/ to learn how to recognize and avoid social security scams.

Generic Greeting

We repeat this advice often: slow down and give yourself time to review the email in detail. Taking time to examine the sender, message content, and links will show the email is not from a legitimate source.

What to do: Report the email using the report phishing button located on your Outlook toolbar.



Good News

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

Opportunities for Improvement

13 clicked on the link

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.