

## 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.

Notification!!

Government Organization <care@socialsmc.com>  
To [REDACTED]

Reply Reply All Forward Tue 2/24/2026 11:50 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

**CAUTION:** This email originated from outside of Montgomery College. **DO NOT** click on links or open attachments unless you were expecting the email, recognize the sender, and know the content is safe.

**Notification: Your Updated Security Statement**

Dear citizen your Social Security Statement has been streamlined and is easier to read than ever before, thanks to our new design which puts the most useful information up front and at a glance.

**Key Features of Your Updated Statement**

- Verification of your earnings record to ensure accuracy and address any discrepancies.
- Personalized monthly retirement benefit estimates, showing potential benefits from ages 62 to 70.
- New fact sheets tailored to your age group and earnings scenario

Please confirm or update your contact details to ensure you receive all future updates without interruption:

We invite you to use our new application to either update or confirm your contact details, as well as to access and review your redesigned Security Statement.

**Please download app from [socialsecurity.gov/reviewyourstatement](https://socialsecurity.gov/reviewyourstatement)**

With instant and anytime online access, paper Statements will no longer be sent automatically. We encourage you to check your statement at least once a year and contact us with any questions or concerns. Thank you for using our online services. Best Regards.

Help **SLAM THE SCAM !**  
Go to [www.ssa.gov/scam](http://www.ssa.gov/scam)  
To learn signs of a scam and how to avoid a scam

<https://adobeupdates.mycircleonline.com/44e942/9ad15571-cd48-4b72-abde-08a00659b754>  
Click or tap to follow link.

Hover over the link to review the URL

## 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.