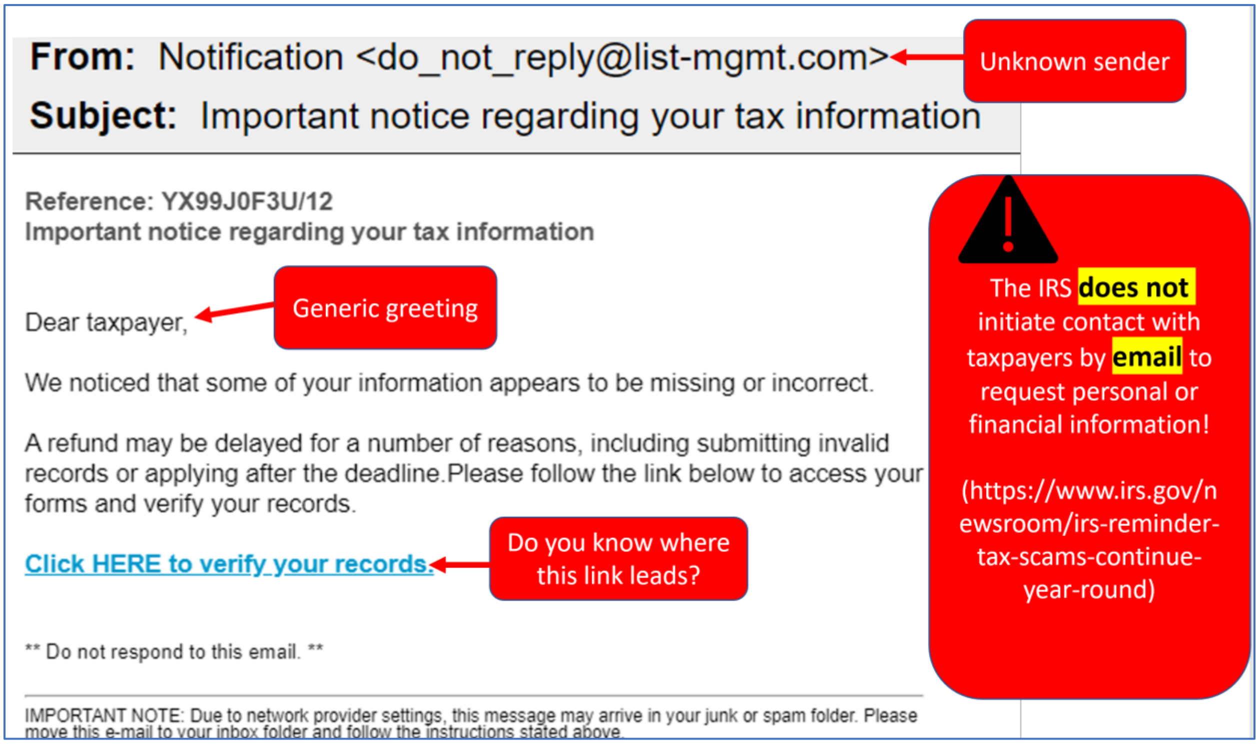
March 2021 Phishing Scenario Results: Tax Information Notice

The Office of Information Technology (OIT) completed a simulated *tax information notice* phishing scenario. This training exercise is a commonly used scam during tax season and uses phrases such as, *refund may be delayed*, to provoke a response from the recipient.

1051 employees reported the phishing scenario to the Phishtrap! Reporting is the preferred action as it provides IT Security the email threat intel it needs to respond.

62 employees clicked the link within the training email. There were several clues within the email to help you identify this message as suspicious. Please review the email again and pay close attention to the red flags:



From: Notification <do_not_reply@list-mgmt.com>

Subject: Important notice regarding your tax information

Unknown sender

Reference: YX99J0F3U/12
Important notice regarding your tax information

Dear taxpayer,

Generic greeting

We noticed that some of your information appears to be missing or incorrect.

A refund may be delayed for a number of reasons, including submitting invalid records or applying after the deadline.Please follow the link below to access your forms and verify your records.

Click HERE to verify your records.

Do you know where this link leads?

** Do not respond to this email. **

IMPORTANT NOTE: Due to network provider settings, this message may arrive in your junk or spam folder. Please move this e-mail to your inbox folder and follow the instructions stated above.

The IRS **does not** initiate contact with taxpayers by **email** to request personal or financial information!

(https://www.irs.gov/newsroom/irs-reminder-tax-scams-continue-year-round)

What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you - **REPORT** the email! Educated employees are our last line of defense to thwart phishing attacks and help us prevent data breaches. The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Complete (or revisit) DataSecurity@MC: Annual Review!

DataSecurity@MC: Annual Review training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. The range of training topics takes about 35 minutes to complete and can be accessed in MC Learns through Workday under the **MC Required Training** category

Below are some common clues to look for in identifying a suspicious email:

- Stay alert to tax related emails – if the email mentions tax forms it is likely a scam. Most tax-related government agencies do not initiate contact by email, text message, or social media. If you filed online, go straight to the servicer's website to check your status.
- Review these Internal Revenue Service (IRS) guidelines to avoid scams https://www.irs.gov/newsroom/irs-reminder-tax-scams-continue-year-round
- Make sure the link to the web address is correct. Do not be misled by sites that claim to be a government agency or tax software company but have a slightly different web address.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- Check your emotions. Do not be curious and investigate the link – **REPORT** the email.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.
- Trust your instincts**.** If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and REPORT it.

If you have any questions or concerns regarding this process, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology