

April 2026 Phishing Results

OIT's April phishing simulation email was titled, *1099-R*. The scenario included a link requesting the recipient to "take a look". This carefully timed phishing email leveraged the April tax filing deadline, creating a brief window for scammers to exploit employees' emotions and sense of urgency, ultimately tricking them into clicking a link to review supposed tax documents.

Clues to Spot in this Scenario:

Issue: Unknown Sender

The sending email address was *Rhan.Thomas@securefilesshares.com*. The email domain is unknown and should not be trusted as an account that would send you tax documents.

What to do:

Do not click on the link to find more information. The best action is to login to your account portal using the web link you have bookmarked. Your account information and associated tax documents should be available within the portal.

Issue: Urgency

The tax filing deadline may be weighing heavily on you if you did not file your taxes. This creates anxiety and may scare you into action.

What to do:

Pause, take the time to think, and do not react in fear. Review the email when you have time and are not in a hurry. Always [report](#) emails that are unexpected and from an unknown sender, especially one that lacks specific content, i.e., tax account identifier.

Take a look at the clues in this scenario:

From: Rhan Thomas <rhan.thomas@securefileshares.com>
Subject: 1099-R

Unknown sender

Good morning,
Kindly take a look at your earliest convenience.

No identifying account information

[1099-R](#)

Thank you.

Warning!
Link destination is
unknown

<http://t.edoctransfer.com/xc107251229/d5741f/63916663-e262-4c5a-952a-2a2ca5325e2c>

INVESTMENTS CONSULTING LLC
24261 IH 15 North #321-327
Austin TX, 78752

****Confidentiality Notice:**** This email and any attachments are intended solely for the recipient and may contain confidential information. If you have received this email in error, please notify the sender immediately by replying to this email and then delete it from your system. Any unauthorized use, sharing, or copying of this message is strictly prohibited.

Good News

654 employees reported the phishing scenario. Great job MC!

Opportunities for Improvement

63 employees clicked 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.