What to look for in IRS email phishing scams

If you receive an official-looking email from what appears to be an official source, whether the IRS or someone in the tax industry, these underlying messages can help determine if it is a scam.

1. If the messages ask for you to update important personal information.
2. If the message asks for you to click a web link to update information.
    - These links may be masked to appear as an official page, but will lead to a scam page.
3. Look out for these subject lines and underlying text referencing:
    - Numerous variations about people's tax refund.
    - Update your filing details, which can include references to W-2.
    - Confirm your personal information.
    - Get my IP Pin
    - Get my E-file Pin.
    - Order a transcript.
    - Complete your tax return information.

The IRS is urging people not to click on these links, but instead to send the email to phishing@irs.gov.

For the complete article and additional resources visit www.IRS.gov

If you have any questions or concerns about emails, websites or unsolicited calls related to Universal 1, please email our Compliance department at **compliance@u1cu.org**. You can also call our eCommerce representatives at **800-543-5000 option 0** or **937-431-3100 option 0**.
We're available **Monday - Friday 8:30 a.m. to 6:00 p.m.** and **Saturday 8:30 a.m. to 12:30 p.m.**