December 3, 2025

Issue Number: 2025-16. The IRS Never Goes Phishing

Phishing is the practice of sending fraudulent communications disguised to appear to be from a reputable source. These attacks, usually through email but increasingly through text messages, are an attempt to try to steal personal and financial information.

The IRS does not request personal or financial information from taxpayers by email. The same is true for other types of electronic communication, such as text messages and use of social media channels.

If you receive a suspicious IRS-related communication:

1. Don't reply to the sender.

2. Don't click, save, or open any attachments. They can contain malicious code that may infect your computer or mobile phone.

3. Don't click on any links. Visit the IRS's identity protection page if you clicked on any links in a suspicious email or website and entered confidential information.

4. Immediately forward the entire message, with the full email headers, to phishing@irs.gov. Don't forward scanned images because this removes valuable information.

5. Delete the original email.

For additional information and resources, please visit Report Phishing and Online Scams.

NOTE: Circular 230 practitioners, tax return preparers, and other tax professionals should also be on guard against phishing generally, as they can be prime targets of fraudsters. See Taxpayers and tax professionals: Beware of these common tax scams | Internal Revenue Service (IRS Tax Tip 2025-30, May 8, 2025):

> **Phishing and spearphishing**
>
> Taxpayers and tax professionals should be alert to fake communications posing as legitimate organizations in the tax and financial community, including the IRS and the states. These messages arrive in the form of an unsolicited text or email to lure victims into providing valuable personal and financial information that can lead to identity theft.
>
> Spearphishing is a tailored phishing attempt targeting a specific individual or group. Tax professionals need to be very careful about spearphishing because of the risk of a data breach. A successful spearphishing attack can ultimately steal client data and the tax preparer's identity, allowing the thief to file fraudulent returns.