Report Phishing and Online Scams

irs.gov/privacy-disclosure/report-phishing

The IRS doesn't ***initiate*** contact with taxpayers by email, text messages or social media channels to request personal or financial information. This includes requests for PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.

What is phishing?

Phishing is a scam typically carried out through unsolicited email and/or websites that pose as legitimate sites and lure unsuspecting victims to provide personal and financial information.

Report all unsolicited email claiming to be from the IRS or an IRS-related function to phishing@irs.gov. If you've experienced any monetary losses due to an IRS-related incident, please report it to the Treasury Inspector General Administration (TIGTA) and file a complaint with the Federal Trade Commission (FTC) through their Complaint Assistant to make the information available to investigators.

NOTE: Please refer to Contact the IRS if you have a tax question not related to phishing or identity theft.

ALERTS:

- W-2 Phishing Scam Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others
- Tax Scams / Consumer Alerts

What to do if you receive a suspicious IRS-related communication

If	Then

You receive an **email** claiming to be from the IRS that contains a request for personal information, taxes associated with a large investment, inheritance or lottery.	1. Don't reply. 2. Don't open any attachments. They can contain malicious code that may infect your computer or mobile phone. 3. Don't click on any links. Visit our identity protection page if you clicked on links in a suspicious email or website and entered confidential information. 4. Forward the email as-is to us at phishing@irs.gov. Don't forward scanned images because this removes valuable information. 5. Delete the original email.
You receive a **phone call** from someone claiming to be from the IRS but you suspect they are not an IRS employee ...	1. Record the employee's name, badge number, call back number and caller ID if available. 2. Call 1-800-366-4484 to determine if the caller is an IRS employee with a legitimate need to contact you. ◦ If the person calling you is an IRS employee, call them back. ◦ If not, report the incident to TIGTA and to us at phishing@irs.gov (Subject: 'IRS Phone Scam')
You receive a **letter, notice or form via paper mail or fax** from an individual claiming to be the IRS but you suspect they are not an IRS employee …	Go to the IRS home page and search on the letter, notice, or form number. Fraudsters often modify legitimate IRS letters. You can also find information at Understanding Your Notice or Letter or by searching Forms and Pubs. • If it is legitimate, you'll find instructions on how to respond or complete the form. • If you don't find information on our website or the instructions are different from what you were told to do in the letter, notice or form, call 1-800-829-1040 to determine if it's legitimate. • If it's not legitimate, report the incident to TIGTA and to us at phishing@irs.gov.
You receive an **unsolicited fax,** such as Form W8-BEN claiming to be from the IRS, requesting personal information …	Please send us the email or scanned fax via email to phishing@irs.gov (Subject: 'FAX'). Visit the FATCA home page and Form W8-BEN for more information.
You receive an **unsolicited telephone call or email, involving a stock or share purchase**, that involves suspicious IRS or Department of Treasury documents such as "advance fees" or "penalties" ...	**... and you are a U.S. citizen located in the United States or its territories or a U.S. citizen living abroad.** **... and you are not a U.S. citizen and reside outside the United States.**
You discover a **website** on the Internet that claims to be the IRS but you suspect it is bogus …	**... send the URL of the suspicious site** to phishing@irs.gov (Subject: 'Suspicious Website').

You receive an **unsolicited text message or Short Message Service (SMS)** message claiming to be from the IRS …	1. Don't reply. 2. Don't open any attachments. They can contain malicious code that may infect your computer or mobile phone. 1. Don't click on any links. If you clicked on links in a suspicious SMS and entered confidential information, visit our identity protection page. 3. Forward the text as-is, to us at 202-552-1226. **Note:** Standard text messaging rates apply. 4. If possible, in a separate text, forward the originating number to us at 202-552-1226 5. Delete the original text.

How to identify phishing email scams claiming to be from the IRS and bogus IRS websites

---

What to do if you receive a suspicious email message that doesn't claim to be from the IRS

If	Then
You receive a suspicious phishing email **not claiming to be from the IRS ...**	Forward the email as-is to reportphishing@antiphishing.org.
You receive an **email** you suspect **contains malicious code** or a malicious attachment and you **HAVE** clicked on the link or downloaded the attachment …	Visit OnGuardOnline.gov to learn what to do if you suspect you have malware on your computer.
You receive an **email** you suspect **contains malicious code** or a malicious attachment and you **HAVE NOT** clicked on the link or downloaded the attachment …	Forward the email to your Internet Service Provider's abuse department and/or to spam@uce.gov.

Additional Resources