IRS

IRS Privacy Policy Topics

- Report phishing
- Identity theft
- Protecting your SSN
- Safeguards Program
- Privacy Impact Assessment
- **IRS Privacy Policy Home**

The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

What is phishing?

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

All unsolicited email claiming to be from either the IRS or any other IRS-related components such as the Office of Professional Responsibility or EFTPS, should be reported to phishing@irs.gov.

However, if you have experienced monetary losses due to an IRS-related incident please file a complaint with the Federal Trade Commission through their **Complaint Assistant** to make that information available to investigators.

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 …**	1. **Do not reply.** 2. **Do not open any attachments.** Attachments may contain malicious code that will infect your computer. 3. **Do not click on any links.** If you clicked on links in a suspicious email or phishing website and entered confidential information, visit our identity protection page. 4. Forward the email as-is, to us at phishing@irs.gov. 5. **After you forward** the email and/or header information to us, **delete the original email** message you received. **Note:** Please forward the full original email to us at phishing@irs.gov. Do not forward scanned images of printed emails as that strips the email of valuable information only available in the electronic copy.
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. Please add in the subject line of the email, 'Suspicious website'.
You receive a **phone call** or **paper** **letter via mail** from an individual **claiming to be the IRS** but you suspect they are not an IRS employee …	**Phone call:** 1. Ask for a call back number and employee badge number. 2. Contact the IRS to determine if the caller is an IRS employee with a legitimate need to contact you. 3. If you determine the person calling you is an IRS

	employee with a legitimate need to contact you, call them back. **Letter or notice via paper mail:** 1. Contact the IRS to determine if the mail is a legitimate IRS letter. 2. If it is a legitimate IRS letter, reply if needed. If caller or party that sent the paper letter is **not legitimate,** contact the Treasury Inspector General for Tax Administration at 1.800.366.4484.
You receive an unsolicited **e-mail or fax, involving a stock or share purchase ...**	**... and you are a U.S. citizen located in the United States or its territories or a U.S. citizen living abroad.** 1. Complete the appropriate complaint form with the U.S. Securities and Exchange Commission. 2. Forward email to phishing@irs.gov. Please add in the subject line of the email, 'Stock'. 3. If you are a victim of monetary or identity theft, you may submit a complaint through the FTC Complaint Assistant. **... and you are not a U.S. citizen and reside outside the United States.** 1. Complete the appropriate complaint form with the U.S. Securities and Exchange Commission. 2. Contact your securities regulator and file a complaint. 3. Forward email to phishing@irs.gov. Please add in the subject line of the e-mail, 'Stock'. 4. If you are a victim of monetary or identity theft, you may report your complaint to econsumer.gov.
You receive an unsolicited **fax (such as Form W8-BEN) claiming to be from the IRS, requesting personal information ...**	Contact the IRS to determine if the fax is from the IRS. • If you learn the fax is not from the IRS, please send us the information via email at phishing@irs.gov. In the subject line of the email, please type the word 'FAX'.
You receive a **text message or Short Message Service** (SMS) message claiming to be from the IRS ...	1. Do not reply. 2. Do not open any attachments. Attachments may contain malicious code that will infect your computer or mobile phone. 3. Do not click on any links. If you clicked on links in a suspicious SMS and entered confidential information, visit our identity protection page. 4. Forward the text as-is, to us at 202-552-1226. **Note:** Standard text messaging rates apply. 5. If possible, in a separate text, forward the originating number to us at 202-552-1226 6. After you forward the text, please delete the original text.
You have a tax-related question ... ***Note:*** **Do not submit tax-related questions to phishing@irs.gov.**	If you have a tax-related question, unrelated to phishing or identity theft, please contact the IRS.

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

- Sample of phishing emails
  - First sample of an actual IRS-related phishing e-mail - PDF
  - Second sample of an actual IRS-related phishing e-mail - PDF

- Is it a phishing website posing as the IRS? - PDF
- Sample of FAX scam
  - Sample of recent fax scam requesting EIN - PDF
- Are you a victim of Identity Theft?
  - Contact the Federal Trade Commission
  - Visit the IRS Identity Theft resource page

The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

The IRS does not ...
... request detailed personal information through email. **... send any communication requesting your PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.**

What to do if you receive a suspicious email message that does not 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 related resources**
- The IRS uses new and social media tools to share the latest information on tax changes, initiatives, products and services.
- The IRS also issues customer satisfaction surveys to capture taxpayer and tax practitioner opinions and suggestions for improving our products and services.
- Are you having trouble downloading a **PDF**?

Page Last Reviewed or Updated: 2012-10-18