# Report phishing and online scams



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.

**Avoid Phishing Emails**

Transcript ASL

## What is phishing? (updated Jan. 19, 2024)

Report all unsolicited email - including the full email headers - 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 for Tax Administration (TIGTA), the Federal Trade Commission, and the Internet Crime Complaint Center (IC3). People can also forward the email to your internet service provider's abuse department.

**NOTE:** You can get help with most tax issues online or by phone.

## What to do if you receive a suspicious IRS-related email (updated Jan. 19, 2024)

If 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. Send the full email headers or forward the email as-is to phishing@irs.gov. Don't forward screenshots or scanned images of emails because this removes valuable information.
5. Delete the original email.

## What to do if you receive a suspicious IRS-related telephone call (updated Jan. 19, 2024)

IRS impersonation telephone calls – as well as other types of unwanted calls (e.g., telemarketing robocalls, fake grants, tech support, sweepstakes winnings, etc.) – remain popular scams. Blocking these types of calls is one strategy taxpayers should consider. Easy to install call blocking software for smartphones is available. While the IRS does not endorse any solution or brand, a limited sample of the available options are:

- Consumer Reports
- Consumer Reports Advocacy
- CTIA

If you receive a phone call from someone claiming to be from the IRS but you suspect they are not an IRS employee:

- View your tax account information online or review their payment options at IRS.gov to see the actual amount owed
- If the caller is an IRS employee with a legitimate need to contact you, please call them back using the appropriate online resources

If the individual is not an IRS employee and does not have a legitimate need to contact you and regardless of whether you were a victim of the scam or not, report the incident to the appropriate law enforcement agencies:

- If IRS-related, please report to the Treasury Inspector General for Tax Administration (TIGTA)
- If Treasury-related, please report to the Office of the Treasury Inspector General (TIG) via oigcounsel@oig.treas.gov.

Please report IRS or Treasury-related fraudulent calls to phishing@irs.gov (Subject: IRS Phone Scam).

For any fraudulent call, after listening to the message, do not provide any information and hang up. When you report the fraudulent call, please include:

- The telephone number of the caller (e.g., Caller ID)
- The telephone number you were instructed to call back
- A brief description of the communication

If possible, please include:

- The employee name
- The employee badge number
- The exact date and time that you received the call(s)
- The geographic location and time zone where you received the call if possible

In addition, please consider filing a complaint with:

- The Federal Trade Commission (FTC)
- The Federal Communications Commission (FCC) Consumers should select the "phone" form and then the "Unwanted Calls" under "Phone Issues" and provide details of the call in the description of their complaint.
- Your local attorney general's office via their consumer complaint form (the reporting mechanism will vary by state).

## How do I verify contact from the IRS?

Go to IRS.gov and search on the letter, notice, or form number. Please be aware fraudsters often modify legitimate IRS letters and forms. You can also find information at Understanding your notice or letter or by searching forms and instructions. For additional information please see How to know it's really the IRS calling or knocking on your door.

If it is legitimate, you'll find instructions on how to respond. If the completion of a form is required and it's provided by a questionable contact, you should verify the form is identical to the same form on IRS.gov by searching forms and instructions.

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, please use the appropriate online resources.

Once you have determined that it is not legitimate, report the incident to TIGTA and phishing@irs.gov.

## What if I receive an email requesting W-2 information? (updated Jan. 19, 2024)

Since 2016, phishing@irs.gov has received emails from organizations that have been targeted by the business email compromise (BEC) / business email spoofing (BES) W-2 scam.

There are multiple variants of this scam (e.g., fake invoice, gift card, wire transfer, title/escrow, etc.). Please only contact the IRS for the W-2 variant. You can report the W-2 variant to the IRS – whether you are a victim or not – and should report any BEC/BES variants to the Internet Crime Complaint Center.

If you are a victim of this scam (e.g., you responded by sending the W-2s) please email dataloss@irs.gov and also send the full email headers to phishing@irs.gov (Subject: W-2 Scam).

If you are a recipient of this scam but did not send any information, please send the full email headers to phishing@irs.gov (Subject: W-2 Scam).

If you report the W-2 scam to phishing@irs.gov please clarify if you are a victim.

Please see:

- IR-2016-34, IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s
- IR-2017-10, IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments
- IR-2017-20, Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others
- IR-2017-130, Don't Take the Bait, Step 6: Watch Out for the W-2 Email Scam
- IR-2018-8, IRS, States and Tax Industry Warn Employers to Beware of Form W-2 Scam; Tax Season Could Bring New Surge in Phishing Scheme

## What if I am a tax preparer and I receive or I am a victim of an IRS-related or tax-related email? (updated Jan. 19, 2024)

See How do I verify contact from the IRS?

If you determine that the contact is not legitimate:

- If the scam is IRS-related, report the incident to phishing@irs.gov, the Treasury Inspector General for Tax Administration (TIGTA), the Federal Trade Commission and the Internet Crime Complaint Center (IC3)
- If the scam is tax-related, report to phishing@irs.gov and the Federal Trade Commission

If you are a victim of a security incident, please review Publication 4557 PDF and contact your stakeholder liaison (SL).

For additional guidance please see FTC Data breach guidance: A guide for businesses

## What if I received a solicitation via social media from someone who claims to be from the IRS? (added Jan. 19, 2024)

Please report the added social media account to the appropriate social media provider.

Please include the full URL of the social media account and report the incident to phishing@irs.gov, the Treasury Inspector General for Tax Administration (TIGTA), the Federal Trade Commission, and the Internet Crime Complaint Center (IC3)

## What if I receive an unsolicited email that references the IRS or taxes? (updated Jan. 19, 2024)

Please send the full email headers to phishing@irs.gov and your internet service provider's abuse department.

Report it to the Federal Trade Commission

## What if I receive a suspicious piece of tax-related US mail that is not from the IRS? (added Jan. 19, 2024)

Most letters sent via US mail from the IRS will include a letter or number. See How do I verify contact from the IRS? In some cases the letters might not be from the IRS but from private debt collection agencies.

Other letters might be unsolicited mailers sent from tax debt relief or tax resolution companies. Report these mailers to the United States Postal Service and the Federal Trade Commission The Federal Trade Commission provides guidance for reducing junk mail

Contact your attorney general's office of consumer protection.

## What if I was charged for an employer identification number (EIN) from an online service? (added Jan. 19, 2024)

Contact your credit card company to dispute the charges and report the company to the Federal Trade Commission

The IRS provides information on obtaining an EIN.

## What to do if you receive an unsolicited IRS-related fax

There is a scam that involves a fake Form W8-BEN. If you are a foreign citizen, please visit the FATCA webpage.

Once you have determined that it is not legitimate, report the incident to TIGTA and to phishing@irs.gov (Subject: FAX).

## What to do if you receive an unsolicited solicitation involving a stock or share purchase that involves suspicious IRS or Department of Treasury documents such as "advance fees" or "penalties?" (updated Jan. 19, 2024)

If 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 (Subject: Stock).
3. If you are a victim of monetary or identity theft, you may submit a complaint to the Federal Trade Commission and to the Internet Crime Complaint Center Please see the Federal Bureau of Investigation's Guidance for Cryptocurrency Scam Victims IRS's phishing@irs.gov does **not** assist in the recovery of monetary losses.

If 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 (Subject: Stock).
4. If you are a victim of monetary or identity theft, you may report your complaint to econsumer.gov

## What if I receive an unsolicited text message or Short Message Service (SMS) message claiming to be from the IRS? (updated Jan. 19, 2024)

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. If you clicked on links in a suspicious SMS and entered confidential information, visit Identity Theft Central.
4. Report the message to 7726(SPAM).
5. Please include both the Caller ID and the message body in your email to phishing@irs.gov. Create a new email. Copy the Caller ID from the message and paste into the email. Press and hold on the body of the text message, select Copy, paste into the same email and send to phishing@irs.gov. If you are unable to copy the Caller ID or message body, please forward a screenshot of the message to phishing@irs.gov. A Multimedia Messaging Service (MMS) message may require you to save the attachment and then attach the file saved to an email to phishing@irs.gov.
6. Delete the original text.
7. For more information see the IRS video on fake IRS-related text messages

## What if I receive a phishing email that is not IRS or tax-related? (updated Jan. 19, 2024)

Phishing emails that are not IRS, Treasury and tax-related should **not** be sent to phishing@irs.gov.

If you receive a suspicious phishing email not claiming to be from the IRS, forward the email as-is to reportphishing@antiphishing.org, your internet service provider's abuse department, and to the Federal Trade Commission.

If 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.

If 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.

## What if I want to train my employees on IRS or tax-related phishing emails by conducting a tax-related phishing exercise? (updated Jan. 19, 2024)

The IRS does **not** grant permission to use "IRS" or its logo in phishing exercises whether organizations use a vendor platform or conduct their own exercise using open-source tools.

You are prohibited from using the IRS or any colorable imitation thereof (e.g., IRS, 1rs, etc.) in phishing exercises. Some agencies have published guidance that the name, logo, or insignia of a U.S. government agency cannot be used in a manner that suggests association with or endorsement by the agency or implies endorsement by a government agency, official, or employee.

IRS, Treasury and tax-themed phishing exercises often cause recipients of the exercise to believe that they have some tax-related issue. Some percentage of exercise recipients will try to report or resolve the issue from the exercise with the IRS or with other individuals (e.g., tax preparers) and/or external organizations.

Organizations are encouraged to coordinate with their appropriate human resources and legal departments before conducting a phishing exercise.

Tax-related exercises should not be conducted during tax season.

Before a tax-themed phishing exercise is conducted, the security team should advise employees to forward suspicious emails to the organization's security team.

Organizations and vendors should provide the appropriate (e.g., telephone number and email address) contact information for the group conducting the phishing exercise on exercise landing pages or similar.

Employees should not be directed to forward tax-related exercise emails to phishing@irs.gov or contact external organizations including the IRS, tax professionals, etc.

Tax-related exercises should include a post-notification that the recipients' taxes have **not** been affected.

## Related

*Page Last Reviewed or Updated: 16-Sep-2024*

Share Print