



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?

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 for Tax 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.

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

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. **Forward** - preferably with the full email headers - 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.

What to do if you receive a suspicious IRS-related telephone call



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's Union](#)
- [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](https://www.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) via their online complaint [form](#) .
- 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) via their online complaint [form](#) .
- Federal Communications Commission (FCC) by visiting the [Consumer Complaint Center](#) . 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](https://www.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](https://www.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 to us at phishing@irs.gov .

What if I receive an email requesting W2 information?

Since 2016, phishing@irs.gov has received emails from organizations that have been targeted by the business email compromise (BEC) / business email spoofing (BES) W2 scam.

There are multiple variants of this scam (e.g., wire transfer, title/escrow, fake invoice, etc.). Please only contact the IRS for the W2 variant. You can report the W2 variant to the IRS – whether you are a victim or not – and should also report any BEC/BES variants to the [Internet Crime Complaint Center](#) .

If you are a victim of this (e.g., you responded by sending the W2s) please email dataloss@irs.gov  and also send the full email headers to phishing@irs.gov  (Subject: W2 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: W2 Scam).

If you report the W2 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 W2s](#)

(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?

See “How to verify contact from the IRS”.

If you determine that the contact is not legitimate:

- If the scam is IRS-related, report the incident to [TIGTA](#)  and to us at phishing@irs.gov .
- If the scam is tax-related, report and to us at phishing@irs.gov .

If you are a victim of a security incident, please review [Publication 4557](#)  and contact your [Stakeholder Liaison \(SL\)](#)



For additional guidance please see [FTC Data Breach Guidance: A Guide for Businesses](#)  .

What if I receive an unsolicited email that references the IRS or taxes?

Send to phishing@irs.gov .




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](#) home page.




Once you have determined that it is not legitimate, report the incident to [TIGTA](#)  and to us at 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"

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 through the [FTC Complaint Assistant](#) .


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?

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 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. Delete the original text.


What if I receive a phishing email that is not IRS or tax-related?

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 .

What if I want to train my employees on IRS or tax-related phishing emails by conducting a tax-related phishing exercise?

You are prohibited from using the IRS or any colorable imitation thereof (e.g., IRS, 1rs, etc.). 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.

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

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

State/Local/Federal/Military organizations should coordinate through DHS NCATS.

Additional Resources

[Press releases and more](#)

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.