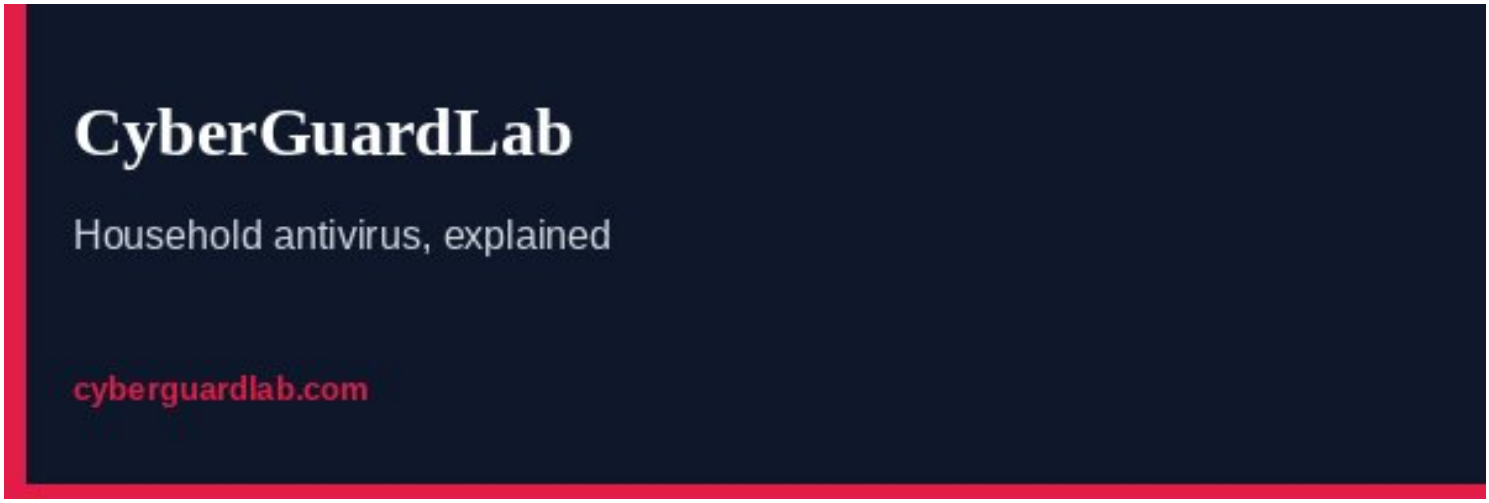
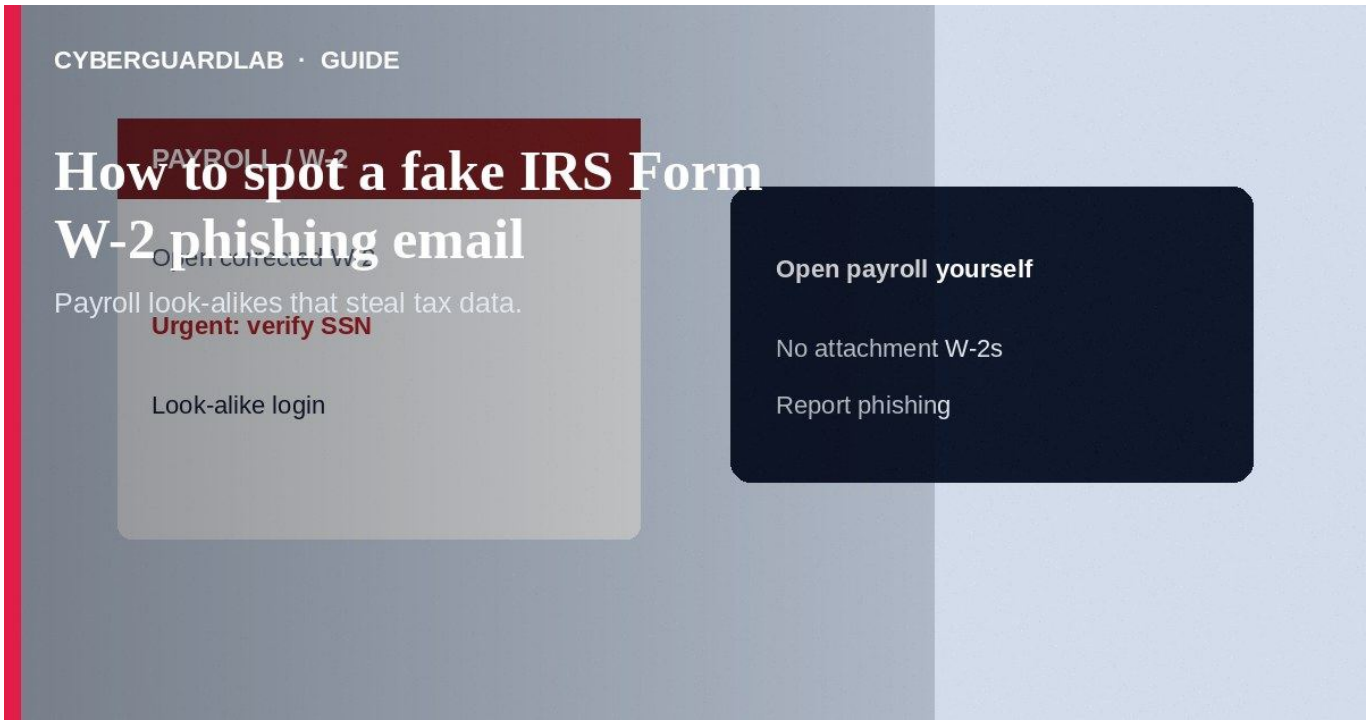


How to spot a fake IRS Form W-2 phishing email

https://cyberguardlab.com/blog/fake-w2-phishing-email

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



A fake IRS Form W-2 phishing email pretends to be payroll, HR, your CPA, or the IRS and urges you to open a "W-2," "corrected wage statement," or "tax transcript" link-or to reply with employee wage files. The goal is malware, credential theft, or a haul of Social Security numbers for identity fraud. The IRS does not email unsolicited W-2 attachments or demand wage files by cold message. Do not open unexpected tax attachments or upload forms to links from email. If you already clicked or sent data, change passwords, freeze credit if SSNs were exposed, and report phishing. This guide is about W-2 and wage-statement phishing-not a phone IRS wage garnishment voice scam, not a general phishing email overview alone, and not credit freeze how-to steps (though freezes help after exposure).

1. How fake W-2 phishing emails work

In tax season-and increasingly year-round-messages say "Your W-2 is ready," "Action required: corrected W-2c," or "CEO needs all employee W-2s today." Links lead to look-alike Microsoft 365, ADP, or IRS pages. Attachments may be .html, .zip,

or Office files with macros. Business email compromise variants spoof a executive and ask payroll staff to email a spreadsheet of W-2s.

Personal variants claim a refund is held until you "verify" with a Form W-2 upload. Real wage statements come through your employer's known payroll portal or paper process-not a surprise public mailbox link.

Shared HR inboxes are prime targets for "send me this year's W-2s" spoofs. Create a written verification rule: no bulk SSN files by ordinary email. Train seasonal tax helpers before January peaks.

2. Red flags before you open or reply

Cue | Likely legitimate | Likely scam

Sender | Employer payroll domain you already use; portal you open yourself | Free email, look-alike domain, or "IRS" cold message with attachment

IRS contact | Mail notices you can verify via IRS.gov instructions; online account you create yourself | Unsolicited email with W-2 download or urgent refund link

Attachments | Expected file types inside a known HR system | Unexpected .zip, .html, or macro documents labeled W-2

Internal ask | Verified ticket or known secure file-transfer process | "CEO" email demanding a full W-2 dump in hours

Login | Bookmark or app you already trust | Link in email to "view statement" that asks for password or MFA codes

Urgency | Normal payroll calendar | "Account locked in 2 hours" or "refund forfeited today"

3. Safer habits (buy-nothing)

* Do not open W-2 attachments or links from unexpected email or SMS.
* Access payroll through the employer site or app you already use-never through a cold link.
* Forward suspected IRS-impersonation phishing to phishing@irs.gov, then delete.

* Payroll staff: verify unusual W-2 export requests by calling the executive on a known number-not by replying to the email.
* Compare general phishing cues in how to spot a phishing email.
* For aggressive IRS phone threats about warrants or gift cards, see IRS wage garnishment scams.

4. If you already clicked or sent data

* Disconnect from the page, run a malware scan, and change passwords for email, payroll, and banking from a clean device.
* Enable two-factor authentication on email and financial accounts.
* If SSNs or employee wage files were sent, notify your employer's security/HR and start IdentityTheft.gov steps; place a credit freeze.
* Report at ReportFraud.ftc.gov and forward the email to phishing@irs.gov.
* Monitor tax accounts via the official IRS online account you open yourself at IRS.gov-not links from the phish.
* Scan your device with a trusted tool such as Norton or Bitdefender. Keep one primary real-time antivirus-avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

FAQ

Does the IRS email W-2 forms to taxpayers?

The IRS does not initiate unsolicited emails with W-2 attachments or demand that you download wage forms from a random link. Employers issue Forms W-2 through their payroll process.

How is this different from an IRS phone garnishment scam?

Phone garnishment scams threaten arrest and demand immediate payment. W-2 phishing focuses on malware and stealing wage/SSN data through email.

Why do criminals want W-2 files?

W-2s contain names, addresses, and SSNs useful for tax refund fraud and new-account identity theft.

Our CFO asked for W-2s by email. Could it be real?

Verify out-of-band. Business email compromise often spoofs executives during tax season.

If you still want a paid suite

Avoiding how to spot a fake IRS Form W-2 phishing email does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* IRS: Tax scams / phishing
* IRS: Email and phishing scams
* FTC ReportFraud
* IdentityTheft.gov
* FTC: Phishing

Also read

* How to spot a phishing email
* How to spot an IRS wage garnishment scam
* How to place a credit freeze at all three bureaus
* How to spot a LinkedIn recruiter phishing scam
* How to report a scam to the FTC