Phishing Awareness Checklist for Tax Offices

IRS #1 Tax Threat · Security Awareness Training
preeminentechnologies.com

Phishing is the #1 way tax office data gets stolen. Train every staff member to recognize, avoid, and report suspicious emails. Post this checklist in your office and review it at the start of every filing season.

■ RED FLAGS — SPOT A PHISHING EMAIL

- ✕ **Urgent subject line demanding action**
  Examples: "Your EFIN will be suspended" — "IRS action required TODAY"
- ✕ **Unexpected sender or spoofed domain**
  irs.gov@suspicious.net is NOT the IRS. Check the full email address.
- ! **Greeting is generic**
  "Dear Taxpayer" or "Dear User" instead of your actual name
- ✕ **Suspicious or mismatched link**
  Hover over any link. The URL showing should match the destination.
- ✕ **Unexpected attachment**
  PDFs, ZIP files, or Word docs you did not request — do not open
- ! **Grammar and spelling errors**
  Legitimate IRS communications are professionally written
- ✕ **Request for sensitive data by email**
  The IRS never asks for SSNs, passwords, or banking info via email
- ✕ **Urgency combined with a reward**
  "Act now to claim your $2,300 tax credit." Legitimate refunds are mailed.

→ BEFORE YOU CLICK ANYTHING

- ! **Pause — do not act under pressure**
  Real agencies give you time. Urgency is a manipulation tactic.
- ✓ **Verify the sender domain carefully**
  irs.gov is the ONLY official IRS domain. No subdomains, no variants.
- ✓ **Hover before you click any link**
  On desktop: hover and read the full URL in the status bar below
- ✓ **Call the sender on a known number**
  Look up the number independently — do not call a number in the email
- ! **Do not download unexpected attachments**
  Even if the sender appears legitimate — confirm by phone first
- ✓ **Check with a colleague before acting**
  A second set of eyes catches what stress makes us miss

■ HOW TO REPORT A SUSPICIOUS EMAIL

- ✓ **Forward to phishing@irs.gov**
  Do NOT click links first. Forward as-is. Then delete.
- ✓ **Report to reportfraud.ftc.gov**
  File a report with the FTC — takes 2 minutes
- ✓ **Tell your office security coordinator**
  Internal reports help protect everyone in the office
- ✓ **Report to your IT provider**
  They can check if the email reached other staff members
- ✓ **Flag in your email client**
  Mark as phishing/spam to help protect others using the same system
- ✕ **Do NOT forward to coworkers "to warn them"**
  Forwarding spreads the threat. Report instead.

! IF YOU ALREADY CLICKED — ACT IMMEDIATELY

- ✕ **Do NOT enter any credentials**
  Close the tab or window immediately without logging in
- ! **Disconnect from the network**
  Unplug ethernet or turn off Wi-Fi to stop potential malware spread
- ✕ **Contact your IT support right now**
  Do not wait. Time matters for containment.
- ! **Change passwords on affected accounts**
  Start with email, tax software, and IRS e-Services
- ! **Contact IRS Stakeholder Liaison**
  Required if you believe taxpayer data may be compromised
- ✓ **Document everything**
  Screenshot the email, note the time, record every action taken
- ! **Notify affected clients if data at risk**
  Most states require notification within 30–90 days

COMMON LURES TARGETING TAX OFFICES

The IRS never initiates contact by email, text, or social media.

- ✕ "Your EFIN has been suspended — verify now"
- ✕ "Client uploaded document — click to view"
- ✕ "IRS refund of $X — provide bank info"
- ✕ "Software license expired — renew here"
- ✕ "Your account will be closed — confirm identity"
- ✕ "New e-file mandate — download form now"