MOST RECENT SCAMS AND HOW TO SPOT THEM

ANY CALLER OR LETTER REQUESTING PAYMENT BY GIFT CARD, WIRE-TRANSFER, CASH APP, OR CRYPTOCURRENCY IS A SCAM.

To freeze your credit in response to fraud, or to be proactive against it, be sure to freeze all three: TransUnion, Equifax, and Experian.

NEW AI-POWERED TAX SCAMS AND INCORRECT TAX ADVICE

Please be aware of new AI scams as the 2026 tax season approaches:

- Attackers can now use AI to "clone" official IRS messages, to the point where letters and voicemails seem 100% accurate and real. These scams can include incredibly detailed information about yourself and/or your family. *SHOULD YOU RECEIVE AN EMAIL, LETTER, OR CALL FROM ANY TAX AGENCY THAT YOU WERE NOT EXPECTING, PLEASE CALL OUR OFFICE TO CONFIRM THE LEGITAMACY OF THE COMMUNICATION.*
- QR Codes, PDFs and Malware: AI has made identifying phishing links, malware, and credential-harvesting pages harder to recognize. Do not click on any link, download any images or documents, or sign in to any portal without confirming the legitimacy beforehand.
- Personal Information Request: If a communication requests your personal information immediately, that is a red flag for a scam.
- Generative AI and "Deepfake" Technologies: Currently making the rounds is an AI phone scam in which the attacker's voice sounds like a family member or friend requesting a transfer of money to help them. This may or may not include a spoofed phone number to verify that person's identity. Using collected data about yourself or the "person" calling though social media platforms, recorded targeted phone calls, public information, and malware-laden Google Drive or OneDrive documents, these calls can appear *very* convincing. Cybercrime consultants suggest using a password with your friends and family in situations like this to confirm the caller's identity.
- AI Threats: IRS and State taxing authorities will never promise a refund, threaten legal action, call and ask for your credit card information, or demand payment through text or email.

Also watch for bad advice from so-called tax experts online and on social media. Much of the information that can be found is incorrect, some of which strongly encourage tax fraud. Please ask about any tax advice you receive or see on social media.

Be aware of the following to spot email scams:

- Different address when hovering over email address;
- Non-IRS or -State email address (legit emails: @*irs.gov* and @*dor.oregon.gov*);
- Indication of a tax refund or money owed (a mailed letter will be sent by the proper tax authorities);
- A link to view documents/information or to verify any information;
- Directing you to a "phishing" website (*IRS.gov* is the official IRS website/ *Oregon.gov/DOR* is the official Oregon Department of Revenue website);
- Emails asking you to update your accounts; and
- Attachments, Images, and QR Codes.

(continued)

Examples of the most recent scams:

- "*This is* [family member's name]. *I need cash for an emergency. Can you Venmo the money to me?"* – This new AI scam uses detailed information pieced together about you or someone you know to convince you to send money somewhere, such as a tow truck company, and will mimic the person's voice and wording.
- *"I accidentally sent the money to your account. Can you return it?"* – This scam involves a stranger sending money to you through a cash app by accident. They will then contact you to ask you to send the money back. Once you do, the money is withdrawn. The issue is that the original money sent to you came from a stolen credit card. The bank or credit card company that flagged the fraud will withdraw that additional amount from your account, leaving you to have to deal with the loss of money and possible issues with money laundering.
- "*You still owe money on your return*" – common phone scam claiming that they are the IRS, or another department, claiming that you owe additional tax. If money is owed, the IRS will send a letter. In this case, please speak to our office prior to sending any money unless it is an expected bill.
- "*Get a large refund by creating your own W-2*" – this ranges from trying to steal your personal information to encouraging you to submit a false W-2.
- "*We calculated your tax refund, and you need to fill out this form*" – this is a very common scam and may also contain malicious links or attachments.
- "*Let us help you sign up for an IRS account*" – common scam to get your personal and log in information.
- "*Let us help you file a casualty loss claim*" – common scam for victims of natural disasters.
- "*We're calling from the FDIC, and we need your bank information*" – the FDIC does not send unsolicited correspondence, ask for sensitive information, threaten, or demand money. Call the FDIC at 1-877-275-3342 if you receive correspondence from someone claiming to be from the FDIC.
- "*Your identity was stolen, and you need gift cards to fix it*" – any call or email, whether for a tax scam or any other scam, requesting/requiring the purchase of gift cards (untraceable currency) is an automatic red flag. No reputable company will use gift cards as a form of payment.
- "*We'll cancel your Social Security number*" or "*You will be arrested/deported*" - do not verify any information; hang up immediately. A social security number cannot be cancelled. Scammers will "spoof"/fake caller ID to show the Department of Justice or a Law Enforcement number to seem legit. Neither legitimate divisions will make a call like this, however, if you are worried, contact your local law enforcement non-emergency line (Deschutes County: 541-693-6911) or your embassy.
- "*This is the Bureau of Tax Enforcement; we're putting a lien or levy on your assets*" - there is no Bureau of Tax Enforcement. Any other initial contact claiming this should be a red flag.
- "*Use this Form W-8BEN to give us personal data*" – while this is a legitimate form, scammers have modified it to ask for personal information and may ask that you fill it out as a "anti-money laundering regulation" or because you were "exempt from tax reporting and withholdings on income.". If you were not in contact with the IRS or another financial institution at the time, do not open the attachments or click the links, and directly call the company in question, or, if claiming to be from the IRS, forward the email as is without opening to phishing@irs.gov.