Tips to Protect your SSN and Identifiable Information

- Keep your card and any other document that shows your Social Security number in a safe place; DO NOT routinely carry your card or other documents that display your number.
- Be careful about sharing your number, even when you are asked for it; ONLY share your SSN when absolutely necessary.
- Protect your personal financial information at home and on your computer.
- Check your credit report annually.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Protect your personally identifiable information; keep it private. Only provide your SSN when YOU initiate the contact or you are sure who you know is asking.

If you've been a victim of a data breach, follow the steps recommended by the Federal Trade Commission's www.identitytheft.gov

If your SSN was compromised, follow the steps outlined in the Taxpayer Guide to Identity Theft.

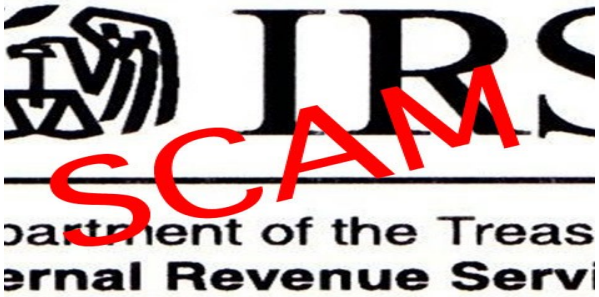
DISPATCH PHONE NUMBER
(307) 527-8700

Cody Police Department

1402 River View Drive
Cody, WY 82414

Phone: 307) 527-8720
Fax: (307) 527-8722

IRS Identity Protection Tips



Stay Vigilant Against Bogus IRS Phone Calls and Emails

IDENTITY PROTECTION TIPS

IRS TAX TIPS

Tax scams take many different forms. Recently, the most common scams are phone calls and emails from thieves who pretend to be from the IRS. They use the IRS name, logo or a fake website to try to steal your money. They may try to steal your identity too. Here are several tips from the IRS to help you avoid being a victim of these tax scams:

The real IRS will not:

- Initiate contact with you by phone, email, text or social media to ask for your personal or financial information.
- Call you and demand immediate payment. The IRS will not call about taxes you owe without first mailing you a bill.
- Require that you pay your taxes a certain way. For example, telling you to pay with a prepaid debit card.

Be wary if you get a phone call from someone who claims to be from the IRS and demands that you pay immediately.

If you don't owe taxes or have nor reason to think that you do:

- Report these calls and other IRS impersonation schemes to the Treasury Inspector General for Tax Administration at 1-800-366-4484 or online at IRS Impersonation Scam Reporting.
- If you discover a website that claims to be the IRS but does not begin with "www.irs.gov," forward the link to phishing@irs.gov.

If you think you may owe taxes:

- Ask for a call back number and an employee badge number.
- Call the IRS at 1-800-829-1040. IRS employees can help you.

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

If you receive and **email** :

- Don't reply
- Don't open any attachments. They can contain malicious code that may infect your computer or mobile phone.
- Don't click on any links. Visit our identity of protection page if you clicked on links in a suspicious email or website and entered confidential information.
- Forward the email as-is at phishing@irs.gov. Don't forward scanned images because this removes valuable information.
- Delete original email.

If you receive a **phone call:**

- Record the employee's name, badge number, call back number and caller ID if available.
- Call 1-800-366-4484 to determine if the caller is an IRS employee with legitimate need to contact you.
    - If the person calling you is an IRS employee, call them back.
    - If not, report the incident to TIGTA and to us at phishing@irs.gov (Subject: IRS Phone Sam')

If you receive a **letter, notice or form via paper mail or fax** claiming to be IRS and you suspect they are not an IRS employee.

- Go to the IRS home page and search on the letter, notice, or form number. Fraudsters often modify legitimate IRS letters. You can also find information at Understanding Your Notice or Letter or searching Forms and Pubs.
- If it is legitimate, you'll find instructions on how to respond or complete the form.
- 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 of form, call 1-800-829-1040 to determine if it's legitimate.
- If it's not legitimate, report the incident to TIGTA and to us at phishing@irs.gov.