FORGE

The Arkansas Cyber Defense Center

IRS/Tax Scam

This involves using the name of the IRS to scam you out of personal information, financial information, or money.

Why be aware?

This scam can be easy to fall for as scammers often pose as representatives of the IRS, which can intimidate people into giving away their financial/personal information and/or money. They may use phishing emails to get your information, or they may promise unrealistic refunds (which you do not receive) to try to get you to pay a small fee.

Red flags:

- Sketchy looking emails with typos and poor grammar
- Asking for personal information before you purchase (email address, SSN, birthdate, etc)
- They contact you unexpectedly
- They threaten to have you arrested if you do not pay now
- Asking for payment using a git card or wire transfer

Immediate actions:

- If you have already provided your financial information, contact your financial institution to see about stopping transactions or canceling accounts.
- If you paid using gift cards or a wire transfer, contact the issuer. They might be able to help you stop the transaction.
- Keep all documentation related to the scam in case you need to file a police report.
- If you provided personal information, like your Social Security number, you may be at risk for identity theft.
- Contact your bank or credit card company to make them aware. Then, contact the three major credit reporting agencies – Experian, TransUnion and Equifax – and place a fraud alert on your credit reports. This will make it harder for the scammer to open new accounts in your name.
- Report any unsolicited email claiming to be from the IRS to phishing@irs.gov.

POWERED BY SBA
U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599