TAX SCAM AWARENESS & PREVENTION

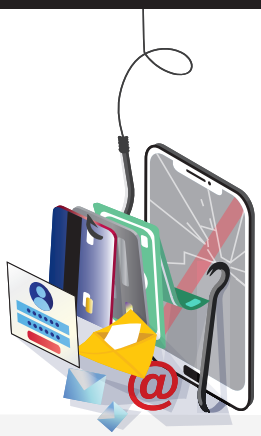
Although tax-related scams are common year-round, they typically increase in numbers during the United States tax season. Each year, scammers are evolving their tactics in an attempt to increase success rates using a variety of lures and methods. Often leading to significant financial loss for victims, identity theft, and account takeovers.

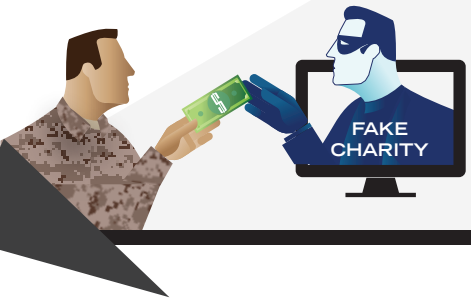
During the tax season, scammers increasingly impersonate the Internal Revenue Service (IRS), TurboTax, and other companies or organizations that provide tax-related services and information to customers.

COMMON SCAM LURES

Scammers use a variety of methods—both traditional and online—to contact and lure victims, including:

- Phone calls
- Phishing emails and text messages
- Fake websites
- Social media platforms
- Physical mail delivery services
- Notifications to file taxes or claim tax refunds
- Prompts to update tax information
- Special discounts on tax services
- Advertisements for quicker refunds
- Tax repayment loans
- Fake W-2 or other tax-related documents



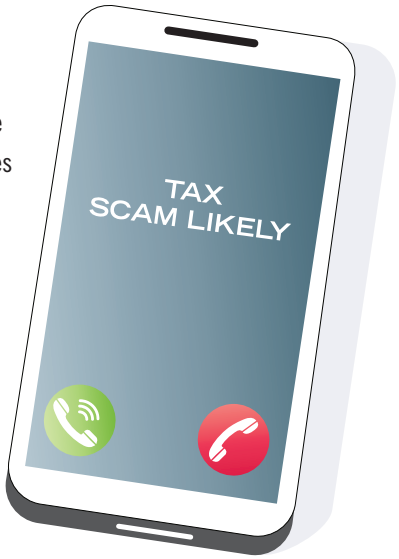


Scammers are increasingly leveraging the abundance of publicly-available information and advanced technology, such as Artificial Intelligence (AI) platforms, to assist in creating scams that are tailored to victims, free of errors, and realistic-looking.

Tax-related scams often include false promises, fake information, and threats to trick victims into making payments to the scammer, providing them with sensitive documents, personal identifiable information (PII), financial data, or account credentials.

TIPS TO SAFEGUARD SENSITIVE INFORMATION

- Keep tax documents in a secure location
- Implement multi-factor authentication (MFA) on accounts when possible
- Use different password and username combinations for different services
- Conduct research on tax companies prior to providing them with sensitive information
- Use complex passwords and change them often
- Go directly to reputable websites for information or tax services, avoid clicking links received by third-party services
- Look for indications that an email, website, or letter is fake, such as spelling and grammar errors, blurry or altered images, or a lack of legitimate contact information
- Refrain from entering sensitive data, such as PII and financial data, into suspicious or unsecure websites or apps



NCIS recommends that DON-affiliated personnel who fall victim to a tax-related scam report incidents to their command or local NCIS office. Personnel may also report suspicious activity to the NCIS Tips Web and Mobile Reporting App at: www.ncis.navy.mil/Resources/NCIS-Tips