



Callaghan Lucerino & Associates LLP
CERTIFIED PUBLIC ACCOUNTANTS

Consumer Alert has been issued by the IRS

Consumer Alerts

Please note that the IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

- If you get an unsolicited email that appears to be from the IRS or a specific IRS component, such as EFTPS, please report it by sending it to phishing@irs.gov.
- If you find a suspicious website that claims to be the IRS, please send the site's URL by email to phishing@irs.gov, using the subject line: suspicious website.

For more information on phishing scams, please see [Protect Your Personal Information](#) and [Suspicious e-Mails and Identity Theft](#).

Don't Fall for Phony IRS Websites

The IRS warns consumers about a new tax scam that uses a website that mimics the IRS e-Services online registration page.

The actual IRS e-Services page offers web-based products for tax preparers, not the general public. The phony web page looks almost identical to the real one.

The IRS gets many reports of fake websites like this. Criminals use these sites to lure people into providing personal and financial information that may be used to steal the victim's money or identity.



Callaghan Lucerino & Associates LLP
CERTIFIED PUBLIC ACCOUNTANTS

IRS Warns Consumers of Possible Scams Relating to Hurricane Sandy Relief

WASHINGTON – The Internal Revenue Service today issued a consumer alert about possible scams taking place in the wake of Hurricane Sandy.

Following major disasters, it's common for scam artists to impersonate charities to get money or private information from well-intentioned taxpayers. Such fraudulent schemes may involve contact by telephone, social media, email or in-person solicitations.

The IRS cautions both hurricane victims and people wishing to make disaster-related charitable donations to avoid scam artists by following these tips:

- To help disaster victims, donate to recognized charities.
- Be wary of charities with names that are similar to familiar or nationally known organizations. Some phony charities use names or websites that sound or look like those of respected, legitimate organizations. The IRS website at IRS.gov has a search feature, Exempt Organizations Select Check, which allows people to find legitimate, qualified charities to which donations may be tax-deductible. Legitimate charities may also be found on the Federal Emergency Management Agency (FEMA) Web site at fema.gov.
- Don't give out personal financial information — such as Social Security numbers or credit card and bank account numbers and passwords — to anyone who solicits a contribution from you. Scam artists may use this information to steal your identity and money.
- Don't give or send cash. For security and tax record purposes, contribute by check or credit card or another way that provides documentation of the gift.
- Call the IRS toll-free disaster assistance telephone number, 1-866-562-5227, if you are a hurricane victim with specific questions about tax relief or disaster related tax issues.

Scam artists can use a variety of tactics. Some scammers operating bogus charities may contact people by telephone to solicit money or financial information. They may even directly contact disaster victims and claim to be working for or on behalf of the IRS to help the victims file casualty loss claims and get tax refunds. They may attempt to get personal financial information or Social Security numbers that can be used to steal the victims' identities or financial resources.

Bogus websites may solicit funds for disaster victims. Such fraudulent sites frequently mimic the sites of, or use names similar to, legitimate charities, or claim to be affiliated with legitimate charities, in order to persuade members of the public to send money or provide personal financial information that can be used to steal identities or financial resources. Additionally, scammers often send e-mail that steers the recipient to bogus websites that sound as though they are affiliated with legitimate charitable causes.

Taxpayers suspecting disaster-related frauds should visit IRS.gov and search for the keywords "Report Phishing."

More information about tax scams and schemes may be found at [IRS.gov](https://www.irs.gov) using the keywords “scams and schemes.”