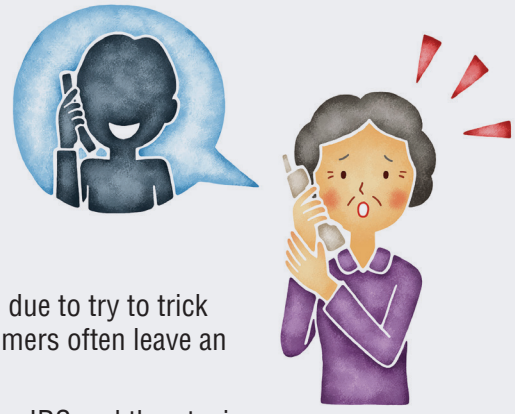
Scam Alerts from Assemblyman Michael Cusick

2018

Protect Yourself: Be Aware of These Common Scams

IRS-Impersonation Telephone Scams



A sophisticated phone scam targeting taxpayers has been making the rounds throughout the country. Callers claim to be IRS employees using fake names and bogus IRS identification badge numbers. They may know a lot about their targets and they usually alter the caller ID to make it look like the IRS is calling.

Victims are told they owe money to the IRS and it must be paid promptly through a gift card or a wire transfer. Victims may be threatened with arrest or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting. Victims may be told they have a refund due to try to trick them into sharing private information. If the phone isn't answered, the scammers often leave an "urgent" callback request.

One of the most common phone scams is the caller pretending to be from the IRS and threatening the taxpayer with a lawsuit or with arrest if payment is not made immediately, usually through a debit card.

Note that the IRS does not:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer. Generally, the IRS will first mail you a bill if you owe any taxes.
- Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand payment without giving you the opportunity to question or appeal the amount they say you owe.
- Ask for credit or debit card numbers over the phone.

If you get a phone call from someone claiming to be from the IRS and asking for money and you don't owe taxes, here's what you should do:

- Do not give out any information. Hang up immediately.
- Contact the **Treasury Inspector General for Tax Administration** at **800-366-4484** to report the scam.
- Report it to the Federal Trade Commission by visiting FTC.gov and clicking on "File a Consumer Complaint." Please add "IRS Telephone Scam" in the notes.
- If you think you might owe taxes, call the **IRS** directly at **1-800-829-1040**.

1911 Richmond Avenue • Staten Island, NY 10314 • 718-370-1384
Room 724, LOB • Albany, NY 12248 • 518-455-5526 • cusickm@nyassembly.gov

Email Phishing

Phishing attacks use email or malicious websites to solicit personal or financial information by posing as a trustworthy organization. Often, recipients are fooled into believing the phishing communication is from someone they trust. A scam artist may take advantage of knowledge gained from online research and earlier attempts to masquerade as a legitimate source, including presenting the look and feel of authentic communications, such as using an official logo. These targeted messages can trick even the most cautious person into taking action that may compromise sensitive data.

The scams may contain emails with hyperlinks that take users to a fake site. Other versions contain PDF attachments that may download malware or viruses.

Some phishing emails will appear to come from a business colleague, friend, or relative. These emails might be an email account compromise. Criminals may have compromised a friend's email account and will look to use their email contacts to send phishing emails.

Here are a few steps to take to protect yourself from email phishing:

- Remember, the IRS doesn't initiate spontaneous contact with taxpayers by email to request personal or financial information. This includes text messages and social media channels. The IRS does not call taxpayers with threats of lawsuits or arrests. No legitimate business or organization will ask for sensitive financial information via email. When in doubt, don't use hyperlinks and go directly to the source's main web page. **www.irs.gov**

- Be vigilant, be skeptical, and learn to avoid phishing emails. These emails may suggest a password is expiring or an account update is needed. The criminal's goal is to entice users to open a link or attachment. The link may take users to a fake website that will steal usernames and passwords. An attachment may download malware that tracks keystrokes. Never open a link or attachment from an unknown or suspicious source. Even if the email is from a known source, approach with caution.
- Use security software to protect against malware and viruses. Some security software can help identify suspicious websites that are used by cybercriminals.
- To report this scam, forward the scam email to **phishing@irs.gov**

Cyber Scams

Cybercriminals seek to turn stolen data into quick cash, either by draining financial accounts, charging credit cards, creating new credit accounts, or even using stolen identities to file a fraudulent tax return for a refund.

Here are seven steps to help with online safety and protecting tax returns and refunds in 2018:

- Shop at familiar online retailers. Generally, sites using the "s" designation in "https" at the start of the URL are secure. Look for the "lock" icon in the browser's URL bar.
- Avoid unprotected Wi-Fi. Beware purchases at unfamiliar sites or clicks on links from pop-up ads. Unprotected public Wi-Fi hotspots also may allow thieves to view transactions. Do not engage in online financial transactions if using unprotected public Wi-Fi.
- Learn to recognize and avoid phishing emails that pose as a trusted source such as those from financial institutions or the IRS. These emails may suggest a password is expiring or an account update is needed. The criminal's goal is to entice users to open a link or attachment. The link may take users to a fake website that will steal usernames and passwords. An attachment may download malware that tracks keystrokes.
- Keep a clean machine. This applies to all devices – computers, phones, and tablets. Use security software to protect against malware that may steal data and viruses that may damage files. Set it to update automatically so that it always has the latest security defenses. Make sure firewalls and browser defenses are always active. Avoid "free" security scans or pop-up advertisements for security software.
- Password-protect sensitive data. If keeping financial records, tax returns, or any personally identifiable information on computers, this data should be protected by a strong password. Also, back-up important data to an external source such as an external hard drive. And, when disposing of computers, mobile phones, or tablets, make sure to wipe the hard drive of all information before trashing.
- Use passwords that are strong, long, and unique. Experts suggest a minimum of 10 characters but longer is better. Avoid using a specific word and instead, opt for using a longer phrase. Use a combination of letters, numbers and special characters. Use a different password for each account. Use a password manager, if necessary.

Federal Student Tax

The IRS issued a warning to taxpayers about bogus phone calls targeting students. These are calls from IRS impersonators demanding payment for a non-existent tax, the "Federal Student Tax."

In this trick, scammers try to convince people to immediately wire money to them. If the victim does not fall quickly enough for this fake "federal student tax," the scammer threatens to report the student to the police.

Scam artists frequently masquerade as being from the IRS, a tax company, and sometimes even a state revenue department. Many scammers use threats to intimidate and bully people into paying a tax bill. They may even threaten to arrest, deport, or revoke the driver's license of their victim if they don't get the money.

Some examples of the varied tactics seen this year are:

- Demanding immediate tax payment for taxes owed on a prepaid gift card.
- Soliciting W-2 information from payroll and human resources professionals.
- "Verifying" tax return information over the phone.
- Pretending to be from the tax preparation industry to assist with your taxes.

The IRS urges taxpayers to stay vigilant against these calls and to know the telltale signs of a scam demanding payment.

IRS FBI Themed Ransomware Scam

The Internal Revenue Service made a warning to people to avoid a phishing scheme that impersonates the IRS and the FBI as part of a ransomware scam to take computer data hostage.

The scam email uses the emblems of both the IRS and the Federal Bureau of Investigation. It tries to entice users to select a "here" link to download a fake FBI questionnaire. Instead, the link downloads a certain type of malware called ransomware that prevents users from accessing data stored on their device unless they pay money to the scammers.

Victims should immediately report any ransomware attempt or attack to the FBI at the **Internet Crime Complaint Center, www.IC3.gov**. Forward any IRS-themed scams to **phishing@irs.gov**.

The IRS does not use email, text messages, or social media to discuss personal tax issues, such as those involving bills or refunds.

Victims should immediately report any ransomware attempt or attack to the FBI at the **Internet Crime Complaint Center, www.IC3.gov**. Forward any **IRS-themed scams** to **phishing@irs.gov**.

The IRS does not use email, text messages, or social media to discuss personal tax issues, such as those involving bills or refunds.

For more information regarding this topic or any other community issue, please contact **Assemblyman Cusick** at **718-370-1384** or **cusickm@nyassembly.gov**.

New York State Assembly • Albany, New York 12248

2018

Assemblyman
Michael Cusick

Scam Alerts

Assemblyman Michael Cusick

Scam Alerts

IRS-Impersonation Telephone Scams
Email Phishing
Cyber Scams
Federal Student Tax
IRS FBI Themed Ransomware Scam