Consumer Alert

Bill Schuette
Attorney General

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern. Consumer Alerts are not legal advice, legal authority, or a binding legal opinion from the Department of Attorney General.

Government Imposter Scams

Contact from the government gets your attention. Criminals use legitimate government references and the treat of government action to trick individuals in to taking action that facilitates theft. The initial communication could come in any form—letter, phone call, email, or text message. No matter the form, the goal is the same: to get personal or business information and steal money.

Fake government texts or emails

If you receive a text or email from any source claiming to come from a government agency or employee with an attachment or link asking you to open it or click on it, do not do it until you verify it is authentic. The attachment or link might contain malware. If you click to open the attached file (typically, a zip file) in a government imposter scam, you will open a virus or other malware and infect your computer or mobile device and allow criminals to steal your personal information, monitor your online activity, and commit fraud.

Scammers know that the threat of government action will cause many recipients to open the attachment out of simple curiosity or concern. Always be very cautious of any unsolicited email or text.

Calling on behalf of the IRS

The most frequently reported scam involves criminals who call and claim to be from the IRS and tell consumers they owe taxes. Often the callers leave messages with a phone number to call back that never works or only works for a short period of time, thus thwarting law enforcement efforts to track them. When taxpayers reach the criminal, they are informed the matter is urgent, and if they want to avoid additional penalties or jail, they must pay immediately using a pre-paid debt card, a wire transfer, an iTunes card, or other method that is difficult for law enforcement to trace. The caller ID might show it’s the IRS and the criminal might even provide a badge number. In reality, the caller ID is faked and the caller is a criminal intent on stealing your money.

In fact, if anyone calls you and asks you to pay with a cash-to-cash money transfer, like MoneyGram or Western Union; or with a PIN from a cash reload card like MoneyPak or Vanilla Road; or with a remotely created payment order using your bank account and routing numbers, they are a fraud and it is a scam. Hang up. The Federal Trade Commission recently made it illegal for any telemarketer to accept any of those forms of payments.

If you owe the IRS money, the IRS will first contact you through the mail and there will be no restrictions on how to pay. And the IRS does not accept iTunes cards as a form of payment.

Fake IRS calls are so prevalent that the federal government has a specific IRS Impersonation Scam Reporting website (www.treasury.gov/tigta/contact_report_scam.shtml).

Lottery or sweepstakes winning notices

Another common government imposter scam is when someone contacts you telling you that you have won a federally supervised lottery or sweepstakes. The criminals claim to be from the National Consumer Protection Agency, the non-existent National Sweepstakes Bureau, or even the Federal Trade Commission.

When making contact, the scammer might tell you that you have to pay taxes or service fees before you can collect your prize, or they will insist that you must wire money immediately. In reality, no government agency is involved, and there are no winnings.

Collecting on a fake debt

Another government imposter scam involves a communication threatening to collect a debt. You may get a call or an official-looking letter claiming to be from a debt collector acting on behalf of a law firm or government agency. The scammer will threaten to arrest you or take you to court on the debt and may even have your address and Social Security number.

Always ask for written verification of the debt. Never pay a debt by wiring money or using a pre-paid debit card. Even if you owe a debt, you still have rights under the Fair Debt Collection Practices Act. For more information on debt collection, debt collection scams, and your rights, read the Attorney General's Consumer Alert on Debt Collection & Debt Collection Scams (www.mi.gov/ag/0,4534,7-164-17337_20942-238041--,00.html).

Awarding fake government grants

Criminals also contact consumers and tell them that they have been selected to receive a government grant. To receive the grant money, the scammer explains a "processing fee" must be paid and asks individuals for bank account information. Grants are not benefits or entitlements. A federal grant is an award of financial assistance from a

federal agency to a recipient to carry out a public purpose of support or stimulation authorized by a law of the United States. Note the following:

- No government grant-making agency will make phone calls; send email or letters to solicit money or personal banking information from a potential grant recipient;
- There are no processing fees for federal grants; and
- Federal grants are not issued for personal use, but are intended for institutions and non-profits to carry out projects with a public purpose.

Ways to protect yourself

- **Never send money to someone you do not know**. Criminals often will pressure consumers into sending money by wire or providing numbers from prepaid cards. They ask for these forms of payment because they cannot be traced. If someone claiming to be from the government is calling and asking you to wire money or provide numbers from prepaid card, hang up.
- **Never give someone who calls your personal or financial information**. As a rule of thumb, never give out your bank account, credit card, or Social Security number unless you are positive you know who is on the other end. Providing this information can lead to criminals stealing your identity.
- **Always be suspicious of someone calling and asking for money**. Scammers will often use official-sounding names, agency names, or position titles to make you trust them. No legitimate government official will ever ask you to send money to collect a prize, nor will a government official call to collect a debt. Also be aware that scammers use internet technology to fake legitimate phone numbers. You can't trust caller IDs.
- **If you get an email or pop-up message that asks for personal or financial information, do not reply, or open any attachment or click on any link in the message**. Legitimate companies don't ask for this information by email.
- **Be cautious about opening any attachment or downloading any file from emails** you receive, regardless who sent them. These files can contain viruses or other software that can weaken your computer's security.
- **Don't email personal or financial information**. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "http**S**://" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some criminals have forged ("spoofed") security icons and "https" sites.
- **Install protective anti-virus, anti-spyware, and firewall software, and keep them up-to-date**. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such

unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones, that can effectively reverse the damage, and that updates automatically.

Report government imposters

If you receive suspicious contact from someone claiming to be from the federal government, you can file a complaint with the FTC (https://www.ftccomplaintassistant.gov/#crnt&panel1-1) or call 877-382-4357. When reporting, include the purported agency, what the imposter asks you to do, the phone number, and any other information you can provide. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

If you receive suspicious contact from someone claiming to be from state or local government, report the contact to the actual agency using contact information you know is accurate. The official State of Michigan website (www.mi.gov) provides reliable contact information for State government.

To file a complaint, you may reach the Attorney General's Consumer Protection Division at:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909

517-373-1140
Toll free: 877-765-8388
Fax: 517-241-3771

Attorney General Website (www.mi.gov/ag)
Attorney General Online Complaint form (www.mi.gov/agcomplaint)