



## AVOID FALLING VICTIM TO SCAMS!!

### Advance Fee Lottery Scams - International Lottery Scam Information

#### Overview

Advance fee lottery scams are one of the most common types of Internet fraud. Be wary of any unsolicited message that informs you that you have won a large sum of money in an international lottery. There is no lottery and no prize. Those who initiate a dialogue with the scammers by replying to the lottery scam message will subsequently be asked for advance fees to cover expenses associated with delivery of the supposed "winnings". They may also become the victims of identity theft. Advance fee lottery scams are normally delivered via email and, more lately, via social media messages. They may also occasionally arrive via surface mail or fax.

In a typical advance fee lottery scam, the criminals will send out many thousands of identical messages in the hope of tricking at least a few recipients into believing that they have actually won a large sum of money.

#### How Advance Fee Lottery Scams Work

You receive an unsolicited message, which states that you have won a major prize in an international lottery. Supposedly, your email address, name or nickname was collected online and attached to a random number that was subsequently entered in a draw for the lottery. In order to claim your prize, you are instructed to contact the official "agent" in charge of your case. You are also advised to keep the win confidential for "security reasons". This part of the scam is an initial phish for potential victims. If you respond in any way to the email, the scammers will send further messages or even contact you by phone in an attempt to draw you deeper into the scam.

You may be asked to provide banking details, a large amount of personal information and copies of your driver's license, passport and/or other identity documents. Ostensibly, these requests are to prove your identity and facilitate the transfer of your winnings. However, if you comply with these requests, the scammers may gather enough information to steal your identity.

In due time, the scammers will request some sort of advance fee supposedly to cover administration, legal, insurance, or delivery costs. This type of scam is just a reworking of the classic "[Nigerian advance fee scam](#)", in which scammers also ask for upfront fees to facilitate a supposed business deal of some form. Like other types of advance fee scams, victims who do actually pay the requested fees will probably find that they receive continuing payment demands to cover "unexpected expenses". The requests for money will go on until the victim realizes what is happening or has no further money to send.

The details of lottery scams vary regularly with regard to the name of the lottery itself, the country of origin, the sponsoring organization, the amount of the "prize" and other particulars. The scammers try to add a patina of legitimacy to their claims by mentioning real financial institutions, government departments or well-known companies. They may also provide links to slick looking, but fraudulent websites that are designed to back up information included in the scam emails. If the scammers are successful in establishing a dialogue with a potential victim, they may provide "proof" such as a scanned image of a supposed government official's ID and even photographs of the "winnings" in cash

#### What To Do If You Receive an Advance Fee Lottery Scam Message

If you receive one of these scam emails, it is important that you do not respond to it in any way. The scammers are likely to act upon any response from those they see as potential victims. Although it can be [educational and even entertaining to "bait" advance fee scammers](#), such endeavors should only be attempted under controlled conditions. These scammers are unscrupulous and unpredictable criminals. There have been violent attacks, abductions and even murders associated with advance fee scams and the criminals that run them should not be trifled with. The best thing to do with these scam messages is to simply delete them. > [What To Do If You Have Submitted Information to Lottery Scammers](#)

If you have supplied banking and credit card details, personal information, and/or copies of identity documents such as your driver's license and passport to the scammers, then you could become a victim of identity theft. For details on what to do, read the information about identity theft published by the [Federal Trade Commission](#)

#### What To Do If You Have Already Given Money To Lottery Scammers

Unfortunately, there is probably very little you can do to recover any money you have already sent. The first step is to cease all communication with the scammers and do not, under any circumstances, send them any more money or information. It is not uncommon for advance fee scam victims to fall into an escalation of commitment trap and continue to send money to the scammers even after they have been told they are being conned. This is because victims can become desperate and are unwilling to let go of the vain hope that the scheme that they are involved in is legitimate after all and that they will eventually get their promised windfall.

If you have sent money to scammers, you should inform your local law enforcement agency as soon as possible. Also, take steps to protect your identity by accessing information about identity theft published by the [Federal Trade Commission](#)

## Arrest Warrant Scams

Did you receive a phone call or email from someone claiming to be a sheriff, policeman, a lawyer or bounty hunter, saying they had a warrant for your arrest? The callers, manipulating caller ID to make the number appear to come from the local sheriff's office or jail, tell potential victims they have an outstanding warrant for an unpaid debt, missed jury duty or some minor infraction and that a fine is due. The callers then convince people to make the payments by wiring it through Western Union MoneyGram or buying a prepaid credit card (like Green Dot) and registering it online.

The [Federal Trade Commission \(FTC\)](#), is warning consumers to be on the alert for scam artists posing as police. There are variations of this scam in which the caller tells the victim that there are outstanding warrants for the victim's arrest. The caller claims that the basis of the warrants is non-payment of the underlying loan and/or hacking. If it's the latter, the caller tells the victim that he or she is wanted for hacking into a business' computer system to steal customer information. The caller will then demand payment via debit/credit card; in other cases, the caller further instructs victims to obtain a prepaid card to cover the payment.

### Look for these signs that a caller may be a Fake Arrest Warrant / fake debt collector if he:

- claims that there is a warrant for your arrest. Police do not call first. If you really are in trouble with the law, you will know it. The police will knock on your door or you will receive a certified piece of mail informing you of any legal action that's being taken against you. If you do owe a fine, you will not get a 15 -minute notice to pay it over the phone.
- is seeking payment on a debt for a loan you do not recognize;
- refuses to give you a mailing address or phone number;
- asks you for personal financial or sensitive information; or
- exerts high pressure to try to scare you into paying, such as threatening to have you arrested or to report you to a law enforcement agency.

### What to do:

If you are contacted by someone who is claims there is a warrant for your arrest or is claiming to collect a debt that you do not owe, you should:

- Ask the caller for his name, company, street address, and telephone number.
- Tell the caller that you refuse to discuss any debt until you get a written "validation notice."
- Contact your local law enforcement agencies if you feel you are in immediate danger;
- If you gave out information about your bank accounts or credit cards, contact your bank(s) and credit card companies;
- Contact the three major credit bureaus and request an alert be put on your file;
- If you have received a legitimate loan and want to verify that you do not have any outstanding obligation, contact the loan company directly;
- File a complaint at [www.IC3.gov](http://www.IC3.gov).
- The notice must include the amount of the debt, the name of the creditor you owe, and your rights under the federal Fair Debt Collection Practices Act.

If a caller refuses to give you all of this information, do not pay! Paying a fake debt collector will not always make them go away. They usually make up another debt to try to get more money from you.

### Stop speaking with the caller.

If you have the caller's address, send a letter demanding that the caller stop contacting you, and keep a copy for your files. By law, real debt collectors must stop calling you if you ask them to in writing.

### Do not give the caller personal financial or other sensitive information.

Never give out or confirm personal financial or other sensitive information like your:

- name,
- date of birth,
- bank account,
- credit card, or
- Social Security number

unless you know whom you're dealing with. Scam artists, like fake debt collectors, can use your information to commit identity theft ' charging your existing credit cards, opening new credit card, checking, or savings accounts, writing fraudulent checks, or taking out loans in your name.

### If You Really Do Owe the Debt, Contact your creditor.

If the debt is legitimate ' but you think the collector may not be ' contact your creditor about the calls. Sometimes fake collectors obtain information about real debts. Share the information you have about the suspicious calls and find out who, if anyone, the creditor has authorized to collect the debt.

Report the call. Contact the FTC and your state Attorney General's office with information about suspicious callers. Many states have their own debt collection laws in addition to the federal FDCPA. Your Attorney General's office can help you determine your rights under your state's law.

### DON'T pay unknown debts, without verification!

First, we are unaware of any legitimate debt collectors contacting people by email (how would they even know an email address associated with a debt?) And legitimate debt collectors must, under the Fair Debt Collection Practices Act, send a letter within 5 days of contacting you, stating what the debt is, why it's owed and how much they believe you owe. The recipient then has 30 days to respond by either contesting it in writing or making payment arrangements.