



Better Business Bureau

January 6, 2012

# Press Release

Contact: Reanna Smith-Hamblin  
(502) 588-0043  
Rsmith-hamblin@louisville.bbb.org

## Start With Trust<sup>®</sup>

### **BBB Names Top Ten Scams of 2011**

BBB investigates thousands of scams every year! Our new Scam Source ([www.bbb.org/scam](http://www.bbb.org/scam)) is a comprehensive resource on scam investigations from BBBs around the country, with tips from BBB, law enforcement and others. You can sign up to receive our Scam Alerts by email, and you can also be a scam detective yourself by reporting scams you've discovered. We've divided scams up into nine major categories and picked the top scam in each, plus our Scam of the Year.

#### **Top Job Scam**

BBB sees lots of secret shopper schemes, work-from-home scams, and other phony job offers, but the worst job-related scam can dash your hopes *and* steal your identity. Emails, websites and online applications all look very professional, and the candidate is even interviewed for the job (usually over the phone) and then receives an offer. In order to start the job, however, the candidate has to fill out a "credit report" or provide bank information for direct deposit of their "paychecks." The online forms are nothing more than a way to capture sensitive personal data - and, of course, there is no job, either.

#### **Top Sweepstakes and Lottery Scam**

You've won a whole lot of money, and in order to claim it you have to send us a smaller amount of money. Keep it confidential! This year's top sweepstakes scam was undoubtedly the email claiming to be from Facebook founder Mark Zuckerberg announcing that the recipient was the winner of \$1 million from the popular social networking site. These kinds of scams often use celebrities or other famous names to make their offer seem more genuine. If you aren't sure, don't click on the link. Go directly to the homepage of the company mentioned. If they are really giving away \$1 million, there will be some kind of announcement on their website.

#### **Top Social Media/Online Dating Scam**

On the Internet, it's easy to pretend to be someone you are not. Are you really friends with all of your "Friends" on Facebook? Do you have a lot of personal information on a dating site? With so much information about us online, a scammer can sound like they know you. There are tons of ways to use social media for scams, but one this year really stands out because it appeals to our natural curiosity...and it sounds like it's coming from a friend. Viral videos claiming to show everything from grisly footage of Osama bin Laden's death to the latest celebrity hijinks have shown up on social media sites, often looking as if they have been shared by a friend. When you click on the link, you are prompted to "upgrade your Flash player," but the file you end up downloading contains a worm that logs into your social media account, sends similar messages to your friends, and searches for your personal data.

#### **Top Home Improvement Scam**

Always near the top of BBB complaint data are home improvement contractors who often leave your home worse than they found it. They usually knock on your door with a story or a deal - the roofer who can spot some missing shingles on your roof, the paver with some leftover asphalt who can give you a great deal on driveway resealing. The worst are those who move in after a natural disaster, taking advantage of desperate homeowners who need immediate help and may not be as suspicious as they would be under normal circumstances. Find a contractor you can trust at [www.bbb.org](http://www.bbb.org).

#### **Top Check Cashing Scam**

Two legitimate companies - Craig's List and Western Union - are used for an inordinate amount of scamming these days, and especially check cashing scams. Here's how it works: Someone contacts you via a Craig's List posting, maybe for a legitimate reason like buying your old couch or perhaps through a scam like hiring you as a secret shopper. Either way, they send you a check for more than the amount they owe you, and they ask you to deposit it into your bank account and then wire the difference via Western Union.

**Louisville:**  
844 South 4<sup>th</sup> Street  
Louisville, KY 40203  
(502) 583-6546

**Bowling Green:**  
(270) 843-4443  
[rchambers@bbbkyn.org](mailto:rchambers@bbbkyn.org)

**Lincoln Trail Area:**  
(270) 982-1289  
[cwilliamson@bbbkyn.org](mailto:cwilliamson@bbbkyn.org)

**For more information:**  
1-800-388-2222  
[www.bbb.org](http://www.bbb.org)



# Press Release

Contact: Reanna Smith-Hamblin  
(502) 588-0043  
Rsmith-hamblin@louisville.bbb.org

## Start With Trust<sup>®</sup>

When the original check bounces, you are out whatever money you wired...and you're still stuck with the old couch.

### Top Phishing Scam

"Phishing" is when you receive a suspicious phone call asking for personal information or an email that puts a virus on your computer to hunt for your data. It's almost impossible to avoid them if you have a telephone or an email account. But the most pernicious phishing scam this year disguised itself as official communication from NACHA – the National Automated Clearing House Association – which facilitates the secure transfer of billions of electronic transactions every year. The email claims one of your transactions did not go through, and it hopes you react quickly and click on the link before thinking it through. It may take you to a fake banking site "verify" your account information, or it may download malware to infiltrate your computer.

### Top Identity Theft Scam

There are a million ways to steal someone's identity. This one has gotten so prevalent that many hotels are posting warnings in their lobby. Here's how it works: You get a call in your hotel room in the middle of the night. It's the front desk clerk, very apologetic, saying their computer has crashed and they need to get your credit card number again, or they must have gotten the number wrong because the transaction won't go through, and could you please read the number back so they can fix the problem? Scammers are counting on you being too sleepy to catch on that the call isn't from the hotel at all, but from someone outside who knows the direct-dial numbers for the guest rooms.

### Top Financial Scam

In challenging economic times, many people are looking for help getting out of debt or hanging on to their home, and almost as many scammers appear to take advantage of desperate situations. Because the federal government announced or expanded several mortgage relief programs this year, all kinds of sound-alike websites have popped up to try to fool consumers into parting with their money. Some sound like a government agency, or even part of BBB or other nonprofit consumer organizations. Most ask for an upfront fee to help you deal with your mortgage company or the government (services you could easily do yourself for free), and almost all leave you in more debt.

### Top Sales Scam

The Internet has introduced a whole new way to rip people off. Penny auctions are very popular because it seems like you can get something useful - cameras, computers, etc. - for way below retail. But you pay a small fee for each bid (usually 50¢ to \$1.00) and if you aren't the winner, you lose that money. Winners often are not even the top bidder, just the last bidder when time runs out. Although not all penny auction sites are scams, some are being investigated as online gambling. BBB recommends you treat them the same way you would legal gambling in a casino – know exactly how the bidding works, set a limit for yourself, and be prepared to walk away before you go over that limit.

### Scam of the Year

The BBB phishing scam! Hundreds of thousands, perhaps millions, of people have gotten emails that very much look like an official notice from BBB. The subject line says something like "Complaint Against Your Business," and the instructions tell the recipient to click on a link or open an attachment to get the details. If the recipient does either, a virus is launched on their computer...a virus that can steal banking information, passwords and other critical pieces of information. BBB is working with security consultants and federal law enforcement to track down the source of these emails, and has already shut down dozens of hijacked websites. Anyone who has opened an attachment or clicked on a link should run a complete system scan using reputable anti-virus software. If your computer is networked with others, all machines on the network should be scanned, as well.

**Louisville:**  
844 South 4<sup>th</sup> Street  
Louisville, KY 40203  
(502) 583-6546

**Bowling Green:**  
(270) 843-4443  
[chambers@bbbkyin.org](mailto:chambers@bbbkyin.org)

**Lincoln Trail Area:**  
(270) 982-1289  
[cwilliamson@bbbkyin.org](mailto:cwilliamson@bbbkyin.org)

**For more information:**  
1-800-388-2222  
[www.bbb.org](http://www.bbb.org)