

**CONSUMER  
ALERT:**

**AVOID**



**Phishing**  
and other  
**Financial**  
**Scams**

Massachusetts Bankers Association, Inc.  
73 Tremont Street, Suite 306  
Boston, MA 02108-3906  
Tel: 617-523-7595 / Fax: 617-523-6373  
[www.massbankers.org](http://www.massbankers.org)

**F**inancial institutions and the Massachusetts Bankers Association (MBA) are warning consumers to be on the lookout for financial scammers that want to separate you from your money. These criminals are becoming increasingly sophisticated, using the Internet and other means to bilk billions of dollars from Americans every year. Many victims are senior citizens or un-savvy computer users who need to know how to navigate more safely on the Internet. But anyone can become a victim.

“The vast majority of online financial transactions happen without a hitch and are quite safe,” says Daniel J. Forte, president of the Massachusetts Bankers Association. “However, fraud can occur, and consumers need to know how to protect themselves to the best of their abilities.”

There are many scams and variations, but what follows are a few of the more common scams to avoid:

**Phishing:** Criminals have gone “phishing.” This is the act of sending pretext emails to unsuspecting recipients who may think it is an email from their own bank or credit card company referencing problems with an account or some situation requiring a fast response. The emails are random, but sending millions increases the likelihood that the scammers will reach some consumers who do business with the purported bank. The email or its links will use the bank’s logo and other graphics to give the impression that it is actually the bank sending the email, or “spoofing” it. The communication will then include a request to “verify” social security, account numbers, passwords or other personal information. Don’t provide it. Your bank or credit card company knows this information and does not need to ask you for it. This is a scam. A newer variation of this practice attaches “spyware” to your computer which can record keystrokes and other activity.

**Spoofing:** This malicious act can take several forms but one of the most common vulnerabilities can occur when you make a mistake or a misspelling while typing in your bank’s email address. The site where you are directed may look just like your bank’s Web site, but it is not. If you make this mistake, the password and account information you provide thereafter could be stolen and put your bank accounts at risk. Best advice: Be sure the address is correct before you press the “enter” button.

**The Advance Fee Scam and Variations:** There are numerous variations to this con and fraud but each has one thing in common: they ask consumers to advance some form of money or personal financial information. Don’t do it. Here are a few of the variations:

- **Your Internet Ad:** This scheme often involves a legitimate ad that you place on the Internet, perhaps trying to sell a car, electronics or any pricey item. Someone responds and cites complications with currency exchange or shipping costs, and sends you a check for more than the selling price of the item you are selling. After depositing the cashier's check, you are then instructed to keep a portion of the extra money and wire or send a check for what's left of the overpayment to the buyer's agent/shipper. After you wire the money out of your account you may find that the check you received and deposited was counterfeit. An important rule: If you're selling something, funds should be moving only in one direction—to you. And make sure, after depositing a check and before you release the goods, that your bank has the funds. Don't simply ask



if the check has cleared, verify that the funds are in your account by asking “Have the funds been ‘finally collected?’” A better rule of thumb: If a deal sounds too good to be true, it probably is. Another warning: A similar fraud using a counterfeit cashier's check can also occur after an online auction.

- **Foreign emails:** There are many email messages circulating on the Internet that ask for your cooperation to move a large sum of money out of another country -- most often some place in Africa -- and all of them are scams. The scammers pose as bankers, chief auditors, chief security officers, remittance officials, directors of finance, directors of government or bank contract award divisions -- all stating they have access to unclaimed funds, generally inactive or delinquent accounts, with millions waiting to be claimed. Others say they are kin to family members who died natural deaths but unexpectedly, or their relatives were killed in assassinations, military coups, or plane crashes. In all of these bogus scenes, the deceased was rich and the letter writer needs help getting the dead relative's vast fortune out of the county due to local snafus or bureaucracy. Individuals are asked to provide funds to cover various fees and for personal identifiers, such as social security numbers, bank account numbers and other similar data. Often they start out by just asking for your phone or FAX number and then in subsequent communication they ask for your bank account number to wire-in the alleged

funds. Don't give them anything. Money will be wired out of your account. If it sounds too good to be true, it probably is.

- **Prizes, Trips, Lottery Winnings:** This bogus communication can come to you via email, the U.S. Postal Service or over the telephone. There are numerous variations but, again, what they have in common is a request for you to advance funds to receive your prize. The scammers claim you have won the Canadian or some other lottery, you have won a trip or some other windfall and all you have to do is advance a "handling" fee to the sponsor or provide your bank account number. Don't do it. If it sounds too good to be true, it probably is.

**Computer Viruses:** Of all Internet frauds, this one is perhaps the most insidious. You receive an email, perhaps with an attachment titled "I love you," or "call me," or just about anything that piques your curiosity. When you open the email, it attaches a small virus or "keylogger" inside your computer that records keystrokes, log-in names and passwords. And it does so without you knowing it. After you have visited 20 or 30 online banking or financial Web sites, it emails that information back to the criminal sponsor. Best advice: Don't open strange emails.

**Credit and Job Applications:** If you see a credit offer or a job posting online, you can fill out an application or send in a resume. However, don't respond if it asks you for your social security number, bank account information, or other personal info. These can be provided later after you have established contact by phone, or mail, or in-person with the companies and have verified that they are legitimate. Otherwise, you could be providing personal information that could result in the draining of your bank account or the stealing of your identity.

**Banks and law enforcement officials are making strides to catch many of these criminals but they won't be effectively deterred until more people are aware of the scams. If you spot suspicious activity, report it to your bank immediately and place a call to your local police. You can ask them if you should also report it to the FBI or Secret Service. Moreover, it's never been more important to check your statements each month and report irregularities to your bank. Consumers have numerous consumer protections when fraud occurs, but many can work only if the activity is reported in a timely fashion.**

*For more information visit [www.massbankers.org](http://www.massbankers.org) or [www.antiphishing.org](http://www.antiphishing.org)*