



By: Jessica Dabrowski--Andover, NJ

Recognize The Disguise: The truth about deceptive messages

You receive an email from your financial institution asking to validate account information. You spot an ad for an amazing loan offer. An official-looking letter arrives. What do these things have in common? They all could be scams. As technology advances, it becomes harder to distinguish the genuine from the imitation. To protect yourself, you need to know the enemy. Here's the scoop on the usual offenders.

Shady sales

Offense: Advertising products or job opportunities untruthfully.

Method: Too-good-to-be-true ads are placed in print, on TV or online. These clever campaigns entice you to spend money upfront on products or training. They draw you in by offering a once-in-a-lifetime deal or a job where you can make money with little or no experience.

Reported cases:

- **Advanced fee loan schemes:** The scammers promise to secure a loan for a fee. They can't get you a loan and disappear with the fee.
- **Work from home scams:** They promise that you can earn lots of money with little effort from home. They make you pay for equipment or advertising, but either don't provide any real prospects of work or don't pay you.

Take action: Report scams to the Better Business Bureau at bbb.org.

Phishing for info

Offense: Sending unsolicited email that persuades you to reveal personal information, or provide unauthorized access to your computer.

Method: These cons are pros at making emails look legit and use phishing and malware as tools of the trade.

- **Phishing:** An email or instant message that appears to be from a friend or trusted institution and usually contains a link. Click the link, and at a replica website (stolen logo and all) you provide login or account information. The spammer obtains all the info needed to steal your identity.
- **Malicious software (malware):** Software that downloads to your computer when you click a spammer's link. It searches for personal information to transmit back

to the spammer. Some malware turn your computer into a botnet, which sends spam or uses storage space without your knowledge.

Reported cases: Phishing messages have been reported from financial institutions, online payment services, and even the IRS. Even accounts at social networking sites like Facebook have been hacked.

Take action: Don't click a link sent in an unsolicited email and always verify the authenticity of requests. Forward questionable emails to spam@uce.gov, and also notify the institution that is being spoofed by the scammers.

Mail hoax

Offense: Sending deceptive, but authentic-looking, direct mail.

Method: Letters labeled with "Official Business," "Important Notice, or "Winner."

Reported cases

- Prize offers: Pay a fee for shipping, and if you're lucky you might receive the prize (which probably isn't worth the price of a stamp).
- Chain letters: Send money to a person on a list and write your name on the next line. They promise that you'll receive lots of money, but don't believe the hype.

Take action: Report mail fraud to the U.S. Postal Inspection Service at postalinspectors.uspis.gov, or simply toss the letter in the shredder.

Bottom Line: The Federal Trade Commission received 643,195 fraud complaints in 2008. Even the savviest consumers can be fooled. Remember: think twice, protect your information, and take action.

Sources: ftc.gov; postalinspectors.uspis.gov; reuters.com; irs.gov; google.com; microsoft.com; onguardonline.gov; bbb.org

Stats

313,982 identity theft complaints were reported to Federal Trade Commission in 2008.

Source: ftc.gov

Victims paid an average of \$3,403 as a result of fraud in 2008.

Source: ftc.gov

Used with the permission of brass|MEDIA Inc.

brass|MEDIA Inc. licensed content is provided with the understanding that the publisher, copyright holder and organizations distributing the magazine are not rendering investment, financial or other professional advice. Investment and other financial decisions depend on each reader's individual facts and circumstances. You should not make decisions based on information contained in licensed brass content without the advice of a qualified professional.