Consumer Reports MoneyAdviser™

FEBRUARY 2011 • $5 VOL. 8, ISSUE 2 EXPERT • INDEPENDENT • NONPROFIT®

New options in roadside assistance See page 3

in this issue

ILLUSTRATION BY BOB ECKSTEIN

Beware of these scams

10 common tricks and what to do about them.

Whether it's fake checks, bogus products and services, or identity theft, it seems as if there's always someone out there trying to make suckers out of us. In the first six months of 2010, scams reported to the fraud center at the National Consumers League cost victims an average of $810.

It's not always easy to spot a scam, even for savvy consumers. That's why you should always be vigilant and take general precautions. Here are some common schemes.

Merchandise fraud

Say you find a really great deal on a digital camera at an online retailer. But shortly after placing your order, you get a phone call from a company representative trying to sell you extra lenses, a fancy case, and other pricey add-ons. You refuse the high-pressure sales pitch, and later you're notified that the camera is no longer in stock. Or it never arrives.

Nonexistent or misrepresented merchandise on the Internet was the fraud center's top complaint in the first half of 2010, with an average loss of $931. That doesn't include fraud involving online auctions, which ranked eighth.

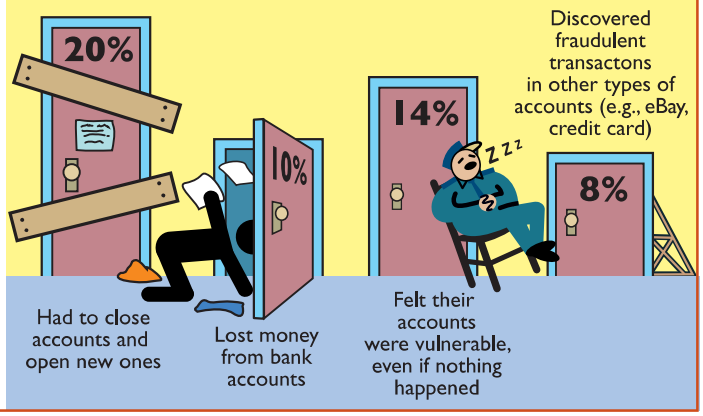
What to do. Check out sellers you're unfamiliar with before buying anything from them. To start, find out whether a company has a report and rating with the Better Business Bureau (*www.bbb.org*).

If you're victimized after paying with cash or by check, you could be out of luck. So use a credit card, especially when buying online or over the phone. If the order doesn't arrive, you can challenge the purchase under federal credit-card rules. Debit-card purchases offer less protection, although some banks volun-

Continued on page 4

Phishing in troubled waters

About 7 percent of Internet-using households responded to phishing scams in 2008 and 2009 (the most recent period for which data are available). Total damage was about $650 million in that period alone. Among the costs to victims:



Source: Consumer Reports National Research Center. Survey results projected to the 82.3 million Internet-using U.S. households.

Common scams

Continued from page 1

tarily provide additional safeguards.

Incidentally, to reduce the risk of unauthorized charges, you might want to consider using a temporary "virtual" or "online" credit-card number, if your bank offers one, for purchases on the Web. In most cases you can request one on the issuer's website. Citibank offers virtual-card software you can install on your computer. You can limit the time the virtual number is active and the maximum amount that can be charged.

Fake checks

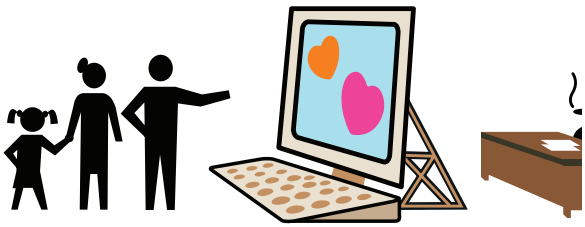
These schemes come under many guises. Bogus checks can be used to pay for something you're selling, such as a used car. Or someone might contact you about a "work at home" opportunity or sweepstakes that you supposedly won. He or she might use a fake check to pay you, with instructions to deposit it and then wire a portion of the proceeds to another party, perhaps to pay "required" fees or taxes. In many cases, these scams involve what appear to be certified or bank checks—but that's no guarantee that they're legitimate. If you deposit or cash a phony check at your bank, it will bounce and your bank will come after you to settle up.

Fake check fraud was the National Consumers League's top scam in 2009; it's now No. 2, representing one in four of the complaint reports that the group receives. The trick costs victims an average of $371.

What to do. Before depositing a check from an unfamiliar source, check with the institution whose name appears on it. And because the bank's contact information on the check could belong to the scammer, search for the institution's phone number and address separately.

Phishing, spoofing, and identify theft

Scammers use e-mail messages, phone calls, and other ways to trick people into revealing their passwords, credit-card and Social Security numbers, and other personal information they can use to steal identities, open credit lines, and the like.



What to do. Don't respond to e-mail messages or phone calls asking for your passwords or other personal information, no matter how urgent the appeal. Instead, contact your bank or other party to see if it made the request. Don't click on hyperlinks you receive in e-mail messages, and carefully type web addresses into your browser to avoid typos. Scammers sometimes set up bogus sites using common misspellings of legitimate web addresses, a practice known as "typosquatting."

Keep your computer's antivirus and antiphishing software up-to-date. And consider using a browser plug-in, such the free McAfee SiteAdvisor *(www.siteadvisor.com)*, which warns about phishing websites and those that transmit viruses.

The grandparent scam

This one comes as a call from a family member, perhaps someone who identifies himself as your grandson, saying he needs help. The story might be that he was in an accident or arrested while traveling outside the country and needs you to wire emergency money, often to Canada. Such calls have cost victims thousands of dollars.

What to do. Don't give money to anyone without verifying his or her identity. If you get a call from a friend or relative asking for help, politely hang up and call the person's home or cell-phone number to find out if they made the call and the emergency is real. You can also call relatives to help determine that the call is legit.

Travel deals with catches

These vacation offers can often be found at fairs and trade shows, or they might come in unsolicited phone calls, faxes, e-mail, or postcards. They're often used to

ILLUSTRATION BY BOB ECKSTEIN

What if you're conned?

Don't just throw up your hands if you're the victim of a scam. Regulatory authorities and agencies might be able to help you, especially if they detect a pattern of complaints. At a minimum, your report can help warn others.

These resources provide information on scams and how to file a complaint:

► **Federal Trade Commission** *(www.ftc.gov)*. The nation's top consumer cop pursues con artists through court and administrative actions, sometimes shutting down deceptive operations and obtaining restitution for victims. Other federal agencies handle complaints in specific areas, such as banking, food, medicine, telecommunications, and travel services. Find them on the Federal Citizen Information Center's website, at *www.pueblo.gsa.gov/complaintresources.htm*. Federal agencies in particular might need to see a pattern of complaints before they take action.

► **State and local officials.** Consumer complaints are usually handled by state attorneys general, state or local consumer protection departments, or a combination of them. The Federal Citizen Information Center has a list of state consumer agencies at *www.consumeraction.gov/state.shtml*. Also check the National Association of Attorneys General *(www.naag.org/current-attorneys-general.php)*. In some states, separate agencies handle complaints about banks, car dealers, insurers, utilities, and licensed professionals. So check your state government's website.

► **U.S. Postal Inspection Service** *(postalinspectors.uspis.gov/)*. It handles mail-related complaints including fraud, theft, and false address changes.

► **Internet Crime Complaint Center** *(www.ic3.gov)*. This is a partnership of the Federal Bureau of Investigation, the National White-Collar Crime Center, and the Bureau of Justice Assistance.

► **Better Business Bureau** *(www.bbb.org)*. With its company reports and alerts, the BBB is a major source of information for consumers and authorities.

entice you to attend sales promotions, say, for a vacation time-share. But some are simply stand-alone offers for trips. Despite the hype, the vacations are usually anything but free or even bargain-priced.

After attending the sales pitch, you might find that you're ineligible for the promised trip because you didn't comply with hidden or hard-to-understand terms and conditions. Available travel dates might be limited and accommodations awful unless you pay for upgrades.

What to do. Forget about this type of vacation. If a business has to offer free trips to generate interest, its products or services probably aren't worth considering.

Poorly disclosed extras

After buying a product or service, you find that you're being charged for something you never meant to order. Maybe it's rustproofing for a new car at a dealership, or a club membership or subscription.

Details about extras might be buried in a contract or a website's fine print. Some companies pass credit-card information to third-parties who are ready to charge the minute customers click an "OK" button online or unknowingly give consent.

What to do. Read everything carefully before you sign or click. Question anything that's unclear, and don't proceed until you're satisfied with the answers.

Phony charities

It could come as e-mail or a phone call urging you to help some cause that might be in the news or tugs at your heartstrings. Some charities are outright frauds; others do little, if anything, to help a cause.

What to do. Don't respond immediately to a solicitation. Instead, check out the group with the major charity watchdogs: the American Institute of Philanthropy (*www.charitywatch.org);* the Better Business Bureau's Wise Giving Alliance (*www.give.org);* and the Charity Navigator (*www.charitynavigator.org*). And make sure you're dealing with the right group. Many con artists use names similar to legitimate charities. For local groups that don't appear on watchdog reports, ask the charity for further information, or donate through a local fundraising federation, such as the United Way, that screens groups.

If you want to help during an emergency, such as a flood or famine, stick with major established charities such as the Red Cross. Charity watchdogs often post names of legitimate groups that help victims.

Health-products fraud

Scammers are always ready to strike after reports of promising dietary supplements and other "medical breakthroughs" hit the news. Websites spring up overnight hawking products—acai berry supplements, for example—even though there's scant evidence of their benefits. The sites might feature celebrity "experts" or phony "reader" comments. Many offer free trials in order to get your credit- or debit-card number and then enroll you in ongoing fee-based programs.

What to do. Buy health products only from companies you know and trust. Double-check the terms and conditions if you're signing up for a free trial that requires you to give payment information.

Sweepstakes scams

Who doesn't want to win a big prize? But if you respond to mail declaring that you're a finalist, or even a winner, the only ones who'll be stuffing their pockets will be the scammers who sent it to you.

Many of these mailings or prize-related phone calls imply that buying something increases your chances of winning. In another variation, you might be told that you have to mail an advance payment to cover taxes, shipping and handling, or other incidental costs of processing or delivering your fabulous prize. Of course, you'll get nothing in return.

What to do. By law, buying services or merchandise can't increase your odds of winning a sweepstakes. Just saying no if you're asked to respond to a prize or sweepstakes promotion will increase your odds—of not getting ripped off.

Advance-fee loans

This one involves companies promising to get you a loan or credit card even if you have bad credit. But after paying the required fee, you might not hear from the company again, or you might be offered a debit or stored-value card. Such offers appear in ads or on websites run by companies that engage in this type of "service." It's illegal for a company doing business by phone to promise a loan and require a fee before it's delivered.

What to do. Avoid companies that promise to get you a loan but don't seem interested in your credit history, the Federal Trade Commission warns. And never pay an advance fee for a loan, even if it's for "insurance," "processing," or "paperwork." $

Red flags for fraud

Along with the specifics mentioned elsewhere in this report, there are some general warning signs that might indicate you're dealing with a scam:

- ► The offer requires you to act quickly.
- ► The company doesn't provide an address or telephone number.
- ► You're told to wire money to a third party, possibly in another country.
- ► An official-looking envelope contains generic words such as "factory alert" or "card-member services," but you've never heard of the company.
- ► You get troubling results when you search the Web using the company name and such words as "review," "complaints," "scam," and "fraud."
- ► The pitch sounds too good to be true, or your instincts otherwise tell you something's suspicious.
- ► If you try navigating away from a website, a pop-up box forces you to confirm your decision to leave, or the site hijacks your browser's "back" button so that clicking it returns you to the same site.

ILLUSTRATION BY BOB ECKSTEIN