

# The sneakiest NEW SHOPPING SCAMS

Easy ways to avoid  
the biggest rip-offs  
online and in stores

Here at ShopSmart, our main job is to help you shop with confidence, whether you're buying turkeys or tires. We do that by giving you the info you need to get the best deals on the best stuff. But just as important as knowing how to sniff out great buys is understanding what it takes to avoid rip-offs. And with Internet fraud on the rise, it's getting tougher to outsmart the criminals.

Complaints to the Internet Crime Complaint Center, a joint operation of the FBI and the National White Collar Crime Center, jumped 22 percent last year. The complaints include plenty of run-of-the-mill scams, like sellers who steal credit-card numbers or take the money and run. But those are child's play compared with what else is brewing.

Think you're too savvy to get taken? OK, maybe you don't fall for those e-mails from Nigerian royalty asking you to wire money, but digital criminals are getting sneakier every year. One scam that can trip up even the most

cautious consumers involves "skimmers" attached to ATMs. Those devices record account numbers and passwords so that thieves can clean out your bank account.

"These guys are constantly thinking of new ways to swindle you, some of which are quite sophisticated," says Brian Krebs, a computer security expert and author of "Krebs on Security" at [Krebsonsecurity.com](http://Krebsonsecurity.com).

Think you're safer shopping at the mall? Official purse-snatching statistics show there's been a downward trend, but many of those crimes aren't reported to law enforcement officials. And pickpocket activity always jumps around holiday time, says Bob Arno, co-author of "Travel Advisory! How to Avoid Thefts, Cons and Street Scams While Traveling" (Bonus Books, 2003). But you can outsmart even the craftiest swindlers if you know what's in their bag of nasty tricks. Here's a guide to the latest, sneakiest scams, and simple tips that can help you protect yourself.

ILLUSTRATIONS: WWW.GREGCLARKE.COM

## The rip-off 'SMISHING'

**How it works** "Phishing" is when you get an e-mail from a supposedly trustworthy source, such as your bank or PayPal, claiming a problem with your account and asking for your user name and password. When you respond, your information is stolen and your account is siphoned. "Smishing" is the latest twist on that scam—instead of getting an e-mail, you get a text message. (The word is a combination of "SMS," for short message service, aka text messaging, and "phishing.") You're told to call a toll-free number, which is answered by a bogus interactive voice-response system that tries to fool you into providing your account number and password.

"It works because people don't give their cell-phone numbers out," Krebs says. "If someone has my cell number, I figure it's someone I know." Thieves can use random-dialing telemarketing services to hit on your number, says Rod Rasmussen, president and CTO of IID, an Internet security firm. If you belong to a credit union, be especially wary—members are targets because often the call-back number has a local area code, not an 800 number, which makes victims less likely to suspect a hoax, Rasmussen says.

**Prevent it!** If you get a text alert about an account, don't respond before you verify that it's legitimate. You can do a Google search on the number to see whether it matches your financial institution. Even better, call the customer-service number at your bank or other service provider to give any needed information to a representative.



## The rip-off Teeny, tiny charges

**How it works** Thieves get hold of your credit- or debit-card number and make very small charges of 20 cents to \$10. The charges appear on your bill with an innocuous-sounding corporate name, and a toll-free number may appear next to the charge. But when you call the number, it's either disconnected or you're instructed to leave a message and your call is never returned.

That was precisely the scam that the Federal Trade Commission broke up in June, according to spokesman Frank Dorman. "We don't know where the thieves got the card numbers, but we're looking into that," he says. The scam was successful because most consumers either didn't

notice the charges or didn't bother to correct them because the amounts were so small. In all, the crime ring racked up more than \$10 million in bogus charges, the FTC estimates.

**Prevent it!** Scrutinize every item on your bill every month, and question those you don't recognize. (Some charges, but not all, will list a phone number.) If you think a charge is fraudulent, notify your card company as soon as possible but no later than 60 days after the charge appears. By law, the card company must remove the disputed amount from your account while it investigates. Worst case, by law you're liable for only the first \$50 on a credit card. (In most cases, Visa and MasterCard will cover the full amount.) Debit cards offer fewer protections: You must report the problem two days after you notice it. If you don't, you could be liable for

the first \$500 in fraudulent charges. If you wait more than 60 days after your statement is mailed, you could lose all the money in your account.

## The rip-off Skimmers

**How they work** Skimmers, devices that thieves attach to ATMs or gas pumps to steal your debit account number and password, have been around for years—and they're not going away. They're getting even more sophisticated.

The devices are placed at the mouth of the card-acceptance slot and record the data off of the magnetic strip on the back of your ATM card when you slide it into the machine. Crooks will usually plant a second device, such as a hidden camera or a transparent plastic PIN pad overlay, that's used to record your PIN when you type it in.

## 3 simple ways to protect yourself

### Sites that can help you stay safe online

**GET THE RIGHT SECURITY SOFTWARE.** In recent tests, we found two great, downloadable programs that protect against viruses, spyware, and other online threats at no charge. Try Avira, at [www.free-av.com](http://www.free-av.com), or Microsoft Security Essentials, at [www.microsoft.com/security\\_essentials](http://www.microsoft.com/security_essentials).

**FIGHT FRAUD.** There are several useful resources for ensuring your online safety. Bookmark these!

■ **FTC.gov.** The Federal Trade Commission's site has lots of fact sheets that tell you what to do if you've been scammed. Under the Consumer Protection tab, click on "Consumer Information" and then "Shopping for Products & Services." Don't miss the helpful primers on what to do if you're billed for merchandise you never receive and "How to right a wrong."

■ **Safeshopping.org.** This site is sponsored by the American Bar Association and is packed with advice



on safe payment methods, protecting your privacy when you shop, and other need-to-know topics.

■ **OnGuardOnline.gov.** This site has tips on Internet shopping and is sponsored by government agencies. Quizzes test your knowledge of spyware, online auctions, ID theft, and more.

■ **Antiphishing.org.** The Anti-Phishing Working Group, an industry-sponsored association, has a tip sheet on how to avoid being scammed. Click on "Consumer Advice," then "How to Avoid Phishing Scams."

**CHECK SELLERS.** Before you do business with anyone, go to the Better Business Bureau, at [www.bbb.org/us](http://www.bbb.org/us). Grades A to F are based on how long the seller has been in business and how good a job it does resolving complaints. Other sites that are worth a look include SiteJabber.com, Complaints.com, and RipoffReport.com, for its user reviews. Also do a Google search of the site or retailer and the word "complaints."



## The rip-off STRIPPED GIFT CARDS

**How it works** Thieves look for gift cards that are displayed on grab-and-go racks, such as in grocery and department stores. They use a handheld scanner—which you can buy online for just a few hundred dollars—to read the code behind the magnetic or scratch-off strip on the back of the card. That, combined with the card number on the front, gives them everything they need to steal the value of the card. Then they put the card back on the rack. Later an unsuspecting buyer purchases the worthless gift card. Even if a card isn't preloaded, a thief can steal the card number and security code, then call the 800 number shown on the card every few days to check the balance. Once a shopper has purchased the card and loaded it with a dollar amount, the thief can spend it before the purchaser does.

**Prevent it!** Buy cards that are behind a customer-service desk, says Tom Browning, vice president of corporate compliance and chief security officer for AlliedBarton Security Services. Inspect the card; if the magnetic or peel-off strip on the back isn't pristine, the card might have been tampered with. When buying a preloaded card, ask the cashier to scan it to make sure the full value is on it. If you're buying from a third-party gift-card site, look at the refund policy. And always hang on to the receipts. If something goes wrong, it can help you—or the gift recipient—get a refund.

In the early days of skimming, the thief had to return to the ATM or gas pump to retrieve the apparatus. But now, Krebs says, wireless technology enables the devices to be rigged to send account information via text message to the thief's cell phone. "The thief can be down the street in a coffee house or halfway around the world," he says. "As long as he's got a working phone signal, he can get the information sent to him right away and start using it."

**Prevent it!** Use credit cards and avoid using non-bank ATMs. Those machines are generally located in areas that are less secure, making it easier for thieves to tamper with them. And

check the card slot: If there's a plastic strip or plastic film sticking out, or anything glued to the card reader, go elsewhere. If your card is stuck inside the card slot, do not leave the machine. Use your cell phone to call your bank branch or the 24-hour service number to report the problem.

### The rip-off

## Membership programs

**How they work** You're buying from a large, reputable website but just before you click the "confirm" button on your purchase, you see a pop-up

window or banner ad with an offer such as "\$10 Cash Back on Your Next Purchase!" Here's the catch. By accepting that so-called deal, you're agreeing to enroll in a Web discount program that's run by a completely separate company. Those programs, which have innocuous names such as "Reservation Rewards," "Travel Values Plus," or "Great Fun," often provide a 30-day trial period during which you get discounts on a variety of merchandise and services. After that, a monthly membership fee, usually \$10 to \$20, will appear on your credit-card bill—even though you never gave that outside company your card number.

Sounds dicey, doesn't it? A Senate

committee headed by Jay Rockefeller, D-W.Va., thought so, too. Last year, the committee launched an investigation into three large companies that sell memberships to those discount clubs: Affinion Group, Vertrue, and Webloyalty. The committee's report was issued last November and alleged, among other things, that "misleading 'Yes' and 'Continue' buttons cause consumers to reasonably think they are completing the original transaction, rather than entering into a new, ongoing financial relationship with a membership club operated by Affinion, Vertrue, or Webloyalty."

The problem is so ubiquitous that in May, Rockefeller introduced a bill to ban that and other misleading sales practices. Meanwhile, the three companies mentioned in the report have pledged to change their ways. Previously, customers' credit-card numbers were provided to the discount company by the original site without the consumer's knowledge. After the investigation began, all three companies started to require consumers to type in, at a minimum, the last four digits of their card number to make it clear that they are entering into a separate transaction. We'll be on the lookout for whether those changes are enough to keep consumers from being duped.

**Prevent it!** Be wary of pop-up windows or banner ads that promise an additional discount before you complete a transaction. If you do click on an offer, take the time to read the fine print. Scrutinize your credit-card statement every month and question any unfamiliar charges, no matter how small. Check your e-mail inbox and spam folder because Web loyalty programs often send a notification e-mail before they start charging your credit card, when you still have time to cancel.

## Hang on to your handbag!

### The holiday shopping season is prime time for pickpockets

Bob Arno, an author and anti-theft consultant, has traveled the world secretly filming pickpockets. So he knows their tricks and how to thwart them. Here's his advice:

■ **GET A GRIP.** Thieves are just as likely to snatch your purse as to slip a hand inside it to grab a wallet. So keep your handbag tight against your body and in front of you at all times. And when you're sitting down in the food court at the mall, don't sling your purse behind you on the chair. Even if you think you're maintaining physical contact with your bag, leaning forward for just a second is all the opportunity a thief needs to grab it. And never put it on the floor, even if it's in front of you.

■ **NIX KNAPSACKS.** They're back in style, but any bag that's not within your view is a juicy target for skilled pickpockets, no matter how securely it's fastened. And avoid purses with open compartments. Bags with zippers are best.

■ **KEEP YOUR FOCUS.** A classic ploy of purse thieves is to create a diversion—pointing at something, talking loudly, holding open a map and asking for directions, or spilling something on your coat then offering to clean it up. It can happen in a restaurant or a busy mall. Whenever anyone approaches you, be sure to firmly hold your purse and keep it in front of you.

■ **PARE DOWN YOUR WALLET.** Do you really need to bring all of your credit cards and ID cards with you? Leave everything except the necessities at home. And never routinely carry around anything with your Social Security number on it. (Photocopy all of the cards in your wallet, just in case.)

■ **BE SMART WITH YOUR CAR.** Park in well-lit areas. If it's still daylight but you plan to shop for a while, park under a street lamp or in a well-lit garage. Always put up your windows and lock the car. If you go back to your car to stow packages, put them in the trunk—visible boxes and bags are magnets for thieves. Don't load up with so many packages that your purse dangles from your arm, out of your sight. Take advantage of curbside pickup or ask the store to hold bags for you. If someone tries to grab your purse, don't resist. "It's not worth losing your life over," Arno says. Also, if you have a GPS device in your car, program it so that your "home" setting isn't your home address. Instead, use the school or church down the street, or crooks will know how to get to your house while you're out. GPS thefts are also on the rise, so don't leave any visible trace of one in your car, including the mount.



### The rip-off

## COUNTERFEIT ELECTRONICS

**How it works** Counterfeiting might seem like old news, but it's still going strong—in fact, stronger than ever. Last year, U.S. Customs and Border Protection made 14,841 seizures of fake and pirated goods worth \$261 billion, an all-time high. The counterfeits seized included the usual suspects—footwear, apparel, and accessories—plus a huge number of electronics. "A knockoff handbag may not present a direct risk to consumers," says Anthony Toderian, spokesman for CSA International, which tests and certifies products, "but counterfeit electronics certainly do." Fake goods could have substandard wiring, faulty fuses, flammable plastic casings, and harmful chemicals such as lead and mercury. All kinds of electronics have been illegally copied, including computers, phones, and handheld gaming devices, he says. Although online shopping and auction sites and deep-discount stores are the

most likely places those fakes will pop up, some have made their way onto the shelves of major retailers. "Buyers for stores can be fooled just as easily as regular consumers can," Toderian says.

**Prevent it!** Look for a label stating that the product has been certified by CSA International or Underwriters Laboratory. (Go to [CSA-International.org](http://CSA-International.org) and click on "Certification Marks" to see what genuine labels look like. At [UL.com](http://UL.com), go to the search box and type in "How to spot fakes.") Look at the product, too. Are there misspellings on the package? If the box is see-through, does it contain all of the listed components, including batteries, cases, and power cords? Is the manufacturer's contact information, including address and phone number, clearly displayed? When in doubt, buy from well-known retailers that offer a full refund.