



THREE WAYS TO PAY IT SAFE

USE THE RIGHT CARD

Pay with a credit card, and by law you'll be liable for no more than \$50 in fraudulent charges. Using a debit card is stickier. Though MasterCard and Visa match the liability cap, the overall legal protections aren't as strong. And once the money is gone from your bank account, you could face delays and hassles in getting it back.

Only 19% of Americans are confident they can tell if a website is safe.

GET A ONE-TIME NUMBER

Several credit card issuers, including Bank of America, Citibank, and Discover, will give you an account number that becomes invalid after one use. (Call customer service to find out more.) If anyone steals that number, it's useless.

WORK WITH A MIDDLEMAN

You can store your credit card or bank account information with a third-party payment system and let that site deal with the store. PayPal is the most widely used; Google Checkout is similar, though fewer sites accept it.

Tech

CYBER-SHOP SAFELY

As the online buying season kicks into high gear, scammers are out in force too. Take these six steps to protect yourself. **By ISMAT SARAH MANGLA**

BE LEERY

Don't open attachments or click on links if they seem at all suspicious. Doing so could let spyware or viruses in. "If you have a shred of doubt about the legitimacy of an attachment, delete it and call the friend who sent it," says Michael Kaiser, executive director of the National Cyber Security Alliance.

INVEST IN PROTECTION

Buy a full suite of security software (\$30 to \$80 a year; top brands include Symantec, McAfee, and Webroot), including antivirus and anti-spyware software. That should help keep out programs that log your keystrokes to steal passwords and financial info.

STAY UP TO DATE

Your web browser and operating system are also vital to protecting your information. Make sure both are configured to get updates from the manufacturer automatically. With a PC, look for a box to check in your preferences or control settings.

GO DIRECT

To steer clear of websites that look like Amazon.com, say, or BestBuy.com but are actually fakes set up to steal your data, don't click on links to get to those e-commerce sites. Type the URL directly into your browser instead.

SCAN FOR SECURITY

Once you're checking out, be sure that you're on a secure page. The address should begin with "https," not "http." The "s" indicates an encrypted connection, so even if your financial information is intercepted, it can't be read. A gold lock on the bottom of the page signals the same thing.

NEVER SHOP IN PUBLIC

Your computer is more vulnerable on a public wireless network—you don't know what security is in place. Adds Murray Jennex, an information systems professor at San Diego State University: "I wouldn't do credit card transactions on a cellphone or via Bluetooth either."