Secure your financial transactions

Whether you're shopping at online auctions or checking a bank balance, you can keep your financial data out of the public eye.

Attention, E-mart shoppers

For the most part, shopping online is a low-risk activity, privacy-wise. That's because most shopping sites use a method of scrambling your credit card number and other information while it travels between your PC and the Web server called SSL (or Secure Sockets Layer); SSL makes it more difficult for someone "listening in" to the data flowing on the wire to intercept these sensitive numbers.

Shopping with a credit card is probably safest. When you use a credit card, you have the legal right to dispute any charge "if the product or service is misrepresented or never delivered," according to a MasterCard International online shopping guide. "If you pay by check or money order, by the time you realize there is a problem, your money will probably be gone."

Still, shopping online isn't completely risk-free. Criminals do indeed troll the Net for unprotected credit card info, addresses, and Social Security numbers. Fortunately, forewarned is forearmed.

Browser encryption

Your credit card info is most vulnerable as it travels across the Net from your computer to an online store. Hackers can intercept your credit card numbers en route by running sniffer software on Web routers that act as traffic signals on the Internet. The *sniffers* can see all the bytes inside a packet and look for keywords such as *password* inside. Fortunately, most modern browsers support Web sites that *encrypt,* or scramble, data in transit. Before you shop, look for sites that say they use SSL encryption (a common standard among reputable e-tailers). When you enter a secure area of a Web site, you should see a small, locked padlock icon at the bottom of your browser window; always check for this when using an online shopping cart. And if at checkout an e-tailer offers to store your credit card information on its servers, just say no. Occasionally, hackers break into store computers and steal that sensitive customer information.

Get the toughest encryption available

Netscape browsers since Navigator 4.61 (the browser portion of Netscape Communicator) ship with 128-bit SSL encryption support (the toughest available). Determine which Netscape version you're currently running by clicking the Help menu in Netscape Navigator and choosing About.

If you use any version of Internet Explorer earlier than 5.5, you'll need to download the 128-bit SSL High Encryption Pack from Microsoft. Internet Explorer 5.5 or later doesn't require this download; all new browsers now ship with 128-bit encryption. You can determine your version by clicking the Help menu in IE and choosing About.

Know your store's reputation

If you're considering shopping from an online retailer for the first time, search the Better Business Bureau's BBBOnLine site first to see if other consumers have reported problems with the company. Also, read the store's shipping, privacy, and return policies to be sure that the site clearly lists the street address and telephone number of its corporate headquarters. (An e-mail address alone isn't sufficient; a real street address can help ensure you're not dealing with a fly-by-night operation.) Sites that claim positive ratings from consumer-friendly organizations such as BBBOnLine or TRUSTe should provide links back to the organization's own site where you can verify the records yourself.

Use a credit card (not a debit card) for purchases

Most banks now offer account holders ATM debit cards that sport a Visa or MasterCard logo. Since these cards function like credit cards, you can use them for most online credit card purchases. However, if someone were to steal your debit card number, he or she wouldn't merely run up a huge credit card debt; the criminal could conceivably drain your entire

checking or savings account before you could say "Stop, thief!" By virtue of the Visa logo on your debit card, banks provide a fraud-protection refund policy (with a $50 deductible) for all cardholders, but it can take several months to get your money back, so it's best to avoid the risk altogether.

Try disposable income

Recently, the members of the credit industry (including American Express and Discover) devised a new tactic to prevent credit card fraud: the disposable credit card number. To get a disposable number, you simply register with your credit card company. Then, whenever you want to make an Internet purchase, you return to your credit company's site and enter the amount of the purchase into a form. The credit card company then provides you with a one-time-only number that you can use for that specific purchase.

Bank safe

If you're considering banking online, you face many of the same issues that online shoppers do. To keep your account information safe as you send it back and forth between your PC and your bank, make sure your bank's Web site uses 128-bit SSL encryption for all transactions. Look for the telltale locked padlock icon; then, before you start using your online account, be sure you're running a browser version that supports SSL (see recommendations above).

You'll also want to make sure that your bank doesn't sell customers' names, addresses, phone numbers, or other sensitive personal information to marketers. This practice exposes you to junk mail and spam. Read your online bank's privacy policy carefully to see who the bank shares information with and ask them to opt you out of any information-sharing programs at the time you sign up for an account. A federal law known as the Gramm-Leach-Bliley act requires financial service companies to provide a way for customers to choose not to let banks sell their customer profiles or to use them for marketing campaigns. If your bank's privacy policy provides Web-based forms that let you opt out of its marketing programs, use them. This may be the only time that filling out a Web form is likely to stop spam from entering your in-box! If your bank doesn't give you an opt-out option, you may want to find another bank.