Fox News

People take risks online with their identity that they'd never dream of taking in the real world. When you hand your credit card to the waiter at an unfamiliar bistro, there's a possibility he'll copy the number and go on a spree with your card. It's not likely, though — too many chances for him to get caught!

Most of us, therefore, don't worry too much about letting a card out of our sight for a short time. But when you give your credit-card number or any sort of personal information to a Web site, you're taking a much more serious chance on identity theft.

Here are a dozen tips, in no particular order, to help keep your identity and personal information safe.

1. **Clam Up.** If a site requires registration, fill in only the required fields. Look closely for at any checkboxes relating to sharing your information — depending on how they're worded, you'll need to check or uncheck the box to deny sharing permission.

2. **Lie.** If the registration isn't part of an important ongoing business relationship, consider filling the required fields with, shall we say, truth-challenged data. Or get ready-made registration information from www.bugmenot.com.

3. **Look for the Lock.** The lock symbol in your browser's Status Bar and "https" in the Address Bar show that you've got a secure connection. Look for it any time you're about to engage in a financial transaction. The lock isn't a guarantee of security, but its absence is a guarantee of NO security.

4. **Sniff Out Phish.** If you get an e-mail about a problem with your bank or other financial institution, never click any links. Go directly to the bank's Web site and research the problem there. If there is no problem, inform the bank about this fraud attempt.

5. **Sniff Out Phish, II.** Internet Explorer 8, Google Chrome, and Firefox 2 include built-in detection of fraudulent Web sites using a combination of **blacklisting** and actual Web-page analysis. Be sure this feature is turned on, and take it seriously.

6. **Search Safely.** For additional help avoiding dangerous Web sites, consider installing one (or more) of the helpful site-safety add-ons described in our Search Securely roundup. If you see a red flag, stay away!

7. **Control Yourself.** Chances are good your security suite includes a **private data protection** option. When the data you've chosen to protect is about to go out in a Web form, e-mail, or IM, it either prevents transmission or replaces the private data. This feature's not for everyone, but if you feel you need help controlling what you send out, give it a try.

8. **Use One-Shot Credit Cards.** Check with your credit card company online — they may offer an option to create one-shot credit card numbers. When you exercise this option to make a purchase online, the number received by the merchant will be valid for just that transaction.

9. **Educate Your Kids.** You can be fanatically careful, but it won't do any good if your kids e-mail or IM personal information to strangers. If they're old enough, get them on your team to protect your family's identity. If not, use parental controls or private data protection to limit their ability to blab family secrets.

10. **Secure Your System.** Forget the Internet — worry about a colleague or neighbor-kid who sits down at your system and copies off your personal files. Use strong passwords, and be sure to lock the desktop when you step away from the computer.

11. **Think Outside the Box.** Don't believe everything that comes in an envelope. And shred any sensitive information before discarding or recycling it. Identity theft isn't limited to the online world!

12. **Inform Yourself.** There are plenty of resources available to help you understand just how you may be vulnerable.