Internet fraud 12401

Technology, Internet

The term " Internet fraud" refers generally to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme. If you use the Internet with any frequency, you'll soon see that people and things online tend to move, as the saying goes, on " Internet time." For most people, that phrase simply means that things seem to happen more quickly on the Internet -- business decisions, information-searching, personal interactions, to name a few - and to happen before, during, or after ordinary " bricks-and-mortar" business hours. Unfortunately, people who engage in fraud often operate in " Internet time" as well. They seek to take advantage of the Internet's unique capabilities -- for example, by sending e-mail messages worldwide in seconds, or posting Web site information that is readily accessible from anywhere in the world - to carry out various types of fraudulent schemes more quickly than was possible with many fraud schemes in the past. Judging by the sheer number of solicitations and " can't miss" propositions that you can see every day in your e-mail mailbox or posted on message boards or Web sites, Internet scams may seem inescapable. While you can't wholly avoid seeing online solicitations that may be fraudulent, here are some tips on how to deal with them. How should you deal with internet fraud? Don't Judge by Initial Appearances. It may seem obvious, but consumers need to remember that just because something appears on the Internet - no matter how impressive or professional the Web site looks - doesn't mean it's true. The ready

availability of software that allows anyone, at minimal cost, to set up a professional-looking Web site means that criminals can make their Web sites look as impressive as those of legitimate e-commerce merchants.

Be Careful About Giving Out Valuable Personal Data Online. If you see e-mail messages from someone you don't know that ask you for personal data - such as your Social Security number, credit-card number, or password - don't just send the data without knowing more about who's asking. Criminals have been known to send messages in which they pretend to be (for example) a systems administrator or Internet service provider representative in order to persuade people online that they should disclose valuable personal data. While secure transactions with known e-commerce sites are fairly safe, especially if you use a credit card, nonsecure messages to unknown recipients are not. Be Especially Careful About Online Communications With Someone Who Conceals His True Identity. If someone sends you an e-mail in which he refuses to disclose his full identity, or uses an e-mail header that has no useful identifying data (e. g., ""), that may be an indication that the person doesn't want to leave any information that could allow you to contact them later if you have a dispute over undelivered goods for which you paid. As a result, you should be highly wary about relying on advice that such people give you if they are trying to persuade you to entrust your money to them. Watch Out for " Advance-Fee" Demands. In general, you need to look carefully at any online seller of goods or services who wants you to send checks or money orders immediately to a post office box, before you receive the goods or services you've been promised. Legitimate startup " dot. com" companies, of course, may not have the

brand-name recognition of long-established companies, and still be fully capable of delivering what you need at a fair price. Even so, using the Internet to research online companies that aren't known to you is a reasonable step to take before you decide to entrust a significant amount of money to such companies.