# Internet crime 12405

Technology, Internet

Internet Crime: The Wave of the Future

Not only has the Internet revolutionized the way we communicate, entertain, and learn, it has forever changed the way we shop, socialize, and conduct business. An estimated 144 million Americans are plugged into cyberspace, and thousands more enter the online world every day. Even if you're not wired, you've heard the buzz, billions of dollars in E-commerce, E-books changing the way we read, and fabulous music libraries acquired for nothing, thanks to Napster and its clones.

The popular image of the WWW is one of earnest geeks and capitalist kids gulping a Starbucks as they sling code. That icon masks something that until recently could only be called the online world's dirty little secret and possibly the biggest threat to modern society. Not only is the web a city filled with endless things to do and sights to see, like any city, it comes with its share of dark, threatening alleys, where not even the most eager explorer would want to end up.

Pornographers and pedophiles on the web, sadly, are nothing new. But because the Internet is so vast and uncharted, the full scope of its dark side has never been fully explored. And the amount of bad stuff out there is truly staggering, rigged auctions, viruses, adoption scams, credit card fraud, and identity theft, to name a few.

The Internet offers several advantages to con artists. One is anonymity. There are no face-to-face encounters. Neither the perpetrator nor the victim can see the other, hear the other s voice, or know the other s age or sex.

Consequently, there are no cues like there would be in a person-to-person context and no chance smell something fishy.

Moreover, the very process of interacting on the Internet, including the informal code of behavior called netiquette, seems to lower consumers' guard. Most people believe that the Internet is a wonderful land of endless information, where nothing bad can happen. That couldn t be any further from the truth.

Much of the fraud seen on the net is of the time-honored variety: pyramid schemes, chain letters, questionable business opportunities, bogus franchises, merchandise and services promised but not delivered, overpriced scholarship search services, work-at-home scams, and phony prizes and sweepstakes. Con artists market their ploys on web sites, in chat rooms and newsgroups, and in E-mail.

And the worst part, everyone is a target. No matter how old or young, how rich or poor, someone is out to get you. Consumers who don't even own a computer may be vulnerable to Internet fraud. Hacker programs can be obtained free on the Web that allow people to generate credit-card numbers using the same algorithms as the ones used by banks. Scammers open accounts with the created numbers, which belong to some cardholder somewhere, and start ordering products online--without even possessing the plastic.

Not surprisingly, law enforcement has its hands full with this new medium. Proving who is behind the computer screen can be difficult, since physical

clues like fingerprints don't exist online--and electronic trails may or may not exist. What makes law enforcement officials jobs even more trying is the fact the their computer skills are way behind those of the internet bandits, and with each step they take, the criminals seem to take two.

As more people get hooked up and as more criminals go online, we will see ever more sophisticated computer crimes. The key to catching these perps is to get them before they strike. All law enforcement officials, not just specialists, should be trained in computers and computer related crimes. Teams and committees should be formed not only to catch Internet crooks but to find out how they operate and possibly predict who and when they ll strike. The focus needs to be taken off the popular street crimes that seem to fascinate law enforcement personnel of the past and geared toward the crime arena of the future, the Internet.