

Internet Crime Trends

Non-delivery of payment or merchandise. Scams impersonating the FBI. Identity theft.

These were the top three most common complaints made to the joint FBI/National White Collar Crime Center's Internet Crime Complaint Center (IC3) last year, according to its just-released [2010 Internet Crime Report](#). The report also includes a state-by-state breakdown of complaints.

In May 2010, the IC3 marked its 10th anniversary, and by November, it had received its two millionth complaint since opening for business.

Last year, the IC3 received more than 300,000 complaints, averaging just over 25,000 a month. About 170,000 complaints that met specific investigative criteria—such as certain financial thresholds—were referred to the appropriate local, state, or federal law enforcement agencies. But even the complaints not referred to law enforcement, including those where no financial losses had occurred, were valuable pieces of information analyzed and used for intelligence reports and to help identify emerging fraud trends.

So even if you think an Internet scammer was targeting you and you didn't fall for it, file a complaint with the [IC3](#). Whether or not it's referred to law enforcement, your information is vital in helping the IC3 paint a fuller picture of Internet crime.

Additional highlights from the report:

Most victims filing complaints were from the U.S., male, between 40 and 59 years old, and residents of California, Florida, Texas, or New York. Most international complainants were from Canada, the United Kingdom, Australia, or India.

In cases where perpetrator information was available, nearly 75 percent were men and more than half resided in California, Florida, New York, Texas, the District of Columbia, or Washington state. The highest numbers of perpetrators outside this country were from the United Kingdom, Nigeria, and Canada.

After non-delivery of payment/merchandise, scams impersonating the FBI, and identity theft, rounding out the top 10 crime types were: computer crimes, miscellaneous fraud, advance fee fraud, spam, auction fraud, credit card fraud, and overpayment fraud.

The report also contained information on some of the alerts sent out by the IC3 during 2010 in response to new scams or to an increase in established scams, including those involving:

Telephone calls claiming victims are delinquent on payday loans.

Online apartment and house rental and real estate scams used to swindle consumers out of thousands of dollars.

Denial-of-service attacks on cell phones and landlines used as a ruse to access victims' bank accounts.

Fake e-mails seeking donations to disaster relief efforts after last year's earthquake in Haiti.

Over the past few years, the IC3 has enhanced the way it processes, analyzes, and refers victim complaints to law enforcement. Technology has automated the search process, so IC3 analysts as well as local, state, and federal analysts and investigators can look for similar complaints to build cases. Technology also allows law enforcement users who may be working on the same or similar cases to communicate and share information.

Because there are so many variations of Internet scams out there, we can't possibly warn against every single one. But we do recommend this: practice good security—make sure your computer is outfitted with the latest security software, protect your personal identification information, and be highly suspicious if someone offers you an online deal that's too good to be true.