

Reporting Computer Crime

Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement.

The primary federal law enforcement agencies that investigate domestic crime on the Internet include: the Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF). Each of these agencies has offices conveniently located in every state to which crimes may be reported. Contact information regarding these local offices may be found in local telephone directories. In general, federal crime may be reported to the local office of an appropriate law enforcement agency by a telephone call and by requesting the "Duty Complaint Agent."

Each law enforcement agency also has a headquarters (HQ) in Washington, D.C., which has agents who specialize in particular areas. For example, the FBI and the U.S. Secret Service both have headquarters-based specialists in computer intrusion (i.e., computer hacker) cases.

To determine some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of crime, please refer to the following table:

Type of Crime	Appropriate federal investigative law enforcement agencies
Computer intrusion	FBI local office U.S. Secret Service Internet Crime Complaint Center
Password trafficking	FBI local office U.S. Secret Service Internet Crime Complaint Center
Copyright (software, movie, sound recording) piracy	FBI local office if imported, U.S. Immigration and Customs Enforcement Internet Crime Complaint Center
Theft of trade secrets	FBI local office
Trademark counterfeiting	FBI local office if imported, U.S. Immigration and Customs Enforcement Internet Crime Complaint Center
Counterfeiting of currency	U.S. Secret Service
Child pornography or exploitation	FBI local office if imported, U.S. Immigration and Customs Enforcement Internet Crime Complaint Center
Child Exploitation and Internet Fraud matters that have a mail nexus	U.S. Postal Inspection Service Internet Crime Complaint Center
Internet fraud and SPAM	FBI local office U.S. Secret Service (Financial Crimes Division) Federal Trade Commission if securities fraud or investment-related SPAM e-mails,

	Securities and Exchange Commission The Internet Crime Complaint Center
Internet harassment	FBI local office
Internet bomb threats	FBI local office ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	FBI local office ATF local office

The Internet Crime Complaint Center (IC3)

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

Other Government Initiatives to Combat Cybercrime

- The STOP Initiative -- The stopfakes.gov website provides information to consumers and businesses on intellectual property, including information on how to report trade in fake goods.
- Department of Homeland Security's National Infrastructure Coordinating Center: (202) 282-9201 (report incidents relating to national security and infrastructure issues)
- U.S. Computer Emergency Readiness Team (U.S. CERT)
- National Association of Attorney General's Computer Crime Point of Contact List (all state related cyber questions)

Source: United States Department of Justice Computer Crime & Intellectual Property Section.
<http://www.usdoj.gov/criminal/cybercrime/reporting.htm>