US police have arrested 150 alleged cyber criminals this summer, said the US Department of Justice in a statement.

The cyber crime swoop, known as Operation Web Snare, dealt with 150,000 victims, who lost more than $215 million between them. The 160 investigations involved identity theft, fraud, counterfeit software, computer intrusions and other intellectual property crimes.

US Attorney-General, John Ashcroft, said that all lawyers dealing with ID theft should make full use of the new Identity Theft Penalty Enhancement Act to achieve prosecutions.

He added that the crackdown depended heavily on international co-operation. “Operation Web Snare ... shows that America’s justice community is seeking to anticipate, out-think and adapt to new trends in Internet crime. This effort shows how effective law enforcement can be against online crime when all levels of government — domestically and internationally — work together.”

Among the list of cases, six men were charged with an alleged denial-of-service attack. Chief Executive Officer at Orbit Communications, Jay R. Echouafni, allegedly hired computer hackers to launch a denial-of-service assault against Orbit’s competitors. It is believed that the attacks cost the companies $2 million in revenue and defence.

In addition, a Ukrainian man has been indicted for credit card trafficking and wire fraud. Roman Vega allegedly ran a website, www.boafactory.com, which sold counterfeit credit card account information.

Operation Snare is the third big crackdown on cybercrime by US police forces. Two other swoops took place in May and November 2003 with the combined arrests of 255.

The cases involved show the extent to which online criminal activity is increasingly not only multi-jurisdictional, but involves the blending of traditional crimes with various forms of computer crime, said the Department of Justice.

Police say new encrypted P2P network poses threat

A new type of peer-to-peer network, which uses encryption to give anonymity to users is a shield for illegal file sharing, warns law enforcement.

Freenet, the next generation of P2P networks, uses encryption, to cloak users who may distribute illegal files, such as pirated copy or child exploitation images. Users of other current P2P networks, like Kazaa, can be identified when sharing...
In Brief

FTC Issues Antiphishing Guide

The US Federal Trade Commission has issued an antiphishing guide to help consumers avoid disclosing key personal data that criminals could use to steal identities or defraud companies. Key tips include:

• Don’t respond to unsolicited emails.
• Don’t send personal data via email or unsecured websites.
• Check bank and credit card statements for unrecognised transactions.
• Use anti-virus software and update it often.
• Be careful when opening email attachments.

Microsoft to Spend $2M Teaching Security

Microsoft is to spend $2 million over the next two years on university courses and lectures to teach secure computing practice. The programme is part of Microsoft’s Trusted Computing initiative.

Half the money will sponsor security courses in computing science, business, and law faculties on a request for proposal basis. The rest will create five fellowships for “exceptional” new computer scientists.

Insider attacks – easy to do – hard to detect

The US Secret Service and CERT have revealed research on a number of insider attack cases. The study shows that most of the attacks were too easy to carry out and most didn’t involve any technical skill.

IT Specialists, with technical knowledge, committed only 23% of the frauds. One IT specialist wrote loopholes into audit software, which concealed his illegal trades, making it nearly impossible for auditors to spot. The fraudster, who carried out the scam said that problems can arise when “the fox is guarding the henhouse.” The fraudster’s boss was essentially turning a blind eye to the ongoings.

In 61% of cases the frauds were brought to the surface by non-IT security staff, including customers and supervisors. The report recommends that “management must be aware that a common perception about who is likely to be an insider threat may be inaccurate.”

Microsoft is to spend $2 million on security courses, lectures, and fellowships to teach secure computing practice.