

National Infrastructure Protection Center  
“Encourages Heightened Cyber Security as Iraq - US Tensions Increase”  
Advisory 03-002  
February 11, 2003

The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq.

Recent experience has shown that during a time of increased international tension, illegal cyber activity: spamming, web defacements, denial of service attacks, etc., often escalates. This activity can originate within another country, which is party to the tension. It can be state sponsored or encouraged, or come from domestic organizations or individuals independently. Additionally, sympathetic individuals and organizations worldwide tend to conduct hacking activity, which they view as somehow contributing to the cause. As tensions rise, it is prudent to be aware of, and prepare for this type of illegal activity.

Attacks may have one of several motivations:

Political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers.

Political activism or disruptive attacks targeting United States systems by those opposed to any potential conflict with Iraq.

Criminal activity masquerading or using the current crisis to further personal goals.

Regardless of the motivation, the NIPC reiterates such activity is illegal and punishable as a felony. The U.S. Government does not condone so-called "patriotic hacking" on its behalf. Further, even patriotic hackers can be fooled into launching attacks against their own interests by exploiting malicious code that purports to attack the other side when in fact it is designed to attack the interests of the side sending it. In this and other ways patriotic hackers risk becoming tools of their enemy.

During times of potentially increased cyber disruption, owners/operators of computers and networked systems should review their defensive postures and procedures and stress the importance of increased vigilance in system monitoring. Computer users and System Administrators can limit potential problems through the use of "security best practices" procedures. Some of the most basic and effective measures that can be taken are:

Increase user awareness

Update anti-virus software

Stop potentially hostile/suspicious attachments at the E-Mail server

Utilize filtering to maximize security

Establish policies and procedures for responding and recovery

All users should be aware that malicious code (e.g., worms and viruses) can be introduced to spread rapidly by using patriotic or otherwise catchy titles, encouraging users to click on a document, picture, word, etc., which automatically spreads the damaging code. For additional security checklists, please refer to the following sites:

[www.cert.org/security-improvement](http://www.cert.org/security-improvement)

[www.unixtools.com/securecheck](http://www.unixtools.com/securecheck)

[www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp)

[www.sans.org/topten.htm](http://www.sans.org/topten.htm)

The NIPC encourages recipients of this advisory to report computer intrusions and /or other crime to federal, state, or local law enforcement, their local FBI office (<http://www.fbi.gov/contact/fo/fo.htm>) and other appropriate authorities. Recipients may report incidents online to <http://www.nipc.gov/incident/cirr.htm>. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206 or [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov).