



News Release

UNITED STATES AIR FORCE

437th AIRLIFT WING PUBLIC AFFAIRS OFFICE
102 East Hill Blvd., Rm. 223, Charleston AFB, S.C. 29404-5154
Phone: (843) 963-5608, 5588 or 5589 Fax (843) 963-5604

PAO email: edmund.memi@charleston.af.mil
After duty hours, call the base operator or
command post (963-2531) & ask for a PA rep

Release No. 08-03

August 15, 2001

INFOCON SYSTEM WARNS AGAINST ATTACKS ON DOD COMPUTERS

CHARLESTON AIR FORCE BASE, S.C. – The Information Operations Condition system is a structured and coordinated approach to react to adverse attacks on DOD computer and telecommunication systems.

Established by the Secretary of Defense, INFOCON is becoming a more commonplace term around Charleston AFB.

The INFOCON system has five conditions, normal, alpha, bravo, charlie, delta, much like THREATCONs. However, it's important not to get the two confused, according to 2nd Lt. Rodney Bagley, 437th Communications Squadron Help Desk officer in charge.

“People are going to hear more and more about INFOCON,” said Bagley. “They need to differentiate between that and the Force Protection condition. While they have the same condition names, they're totally different.”

Bagley said INFOCON procedures are applied and activated to minimize and reduce disruptions to telecommunication and computer systems and networks. CAFB is currently in INFOCON Alpha.

“The Red Worm virus is our concern right now,” said Bagley. “It seems to target government computers. By going into alpha, we’re in more of a protective posture. When we went into alpha, we ran checklists and followed guidance to keep our systems safe.”

The Air Force Network Operation Center, Kelly AFB, Texas, provides that guidance and advises the base on current INFOCONs, according to Bagley. AFNOC also monitors networks and scans them for suspicious activity.

No matter what the current INFOCON, there are steps computer users can use to protect their systems and the base server against attacks. Running Norton AntiVirus Corporate Edition with the latest definition is the best way to stay protected, according to Staff Sgt. Mike Childers, 437 CS boundary protection specialist.

“You have to be running Realtime Protection for your e-mails to be scanned before you open them,” said Childers. “If Norton detects something in an attachment, it will usually quarantine the e-mail and let you know.”

Childers said some computer systems on base are set up to always run Realtime Protection, but some aren’t. If Realtime is currently active, a small yellow shield icon will be showing on the bottom right corner of the computer screen. If a red circle with a line covers the shield, it is not running. Right clicking the shield and selecting “Enable File System Realtime protection” can turn it on.

Along with Norton, Bagley said unplugging a system from the network at the first sign of something suspicious could prove to be vital. He cited one recent instance when an airman received a suspicious e-mail.

“She unplugged the LAN connection and contacted her workgroup manager,” said Bagley. The manager contacted us, and sure enough, it turned out to be a virus.

“Preparation is the key,” he continued. “As the user on the network, you must ensure you are running the latest virus definition. If you think your system is infected, disconnect from the

network immediately. Don't power it down. Next, report it to your workgroup manager, functional system administrator or the Network Control Center Helpdesk.”

Everyone who uses a government computer should be aware of the INFOCONs and be educated about how to protect this vital government resource.

(For more information, contact Master Sgt. Daniel Murphy at 963-5582 or Staff Sgt. Pamela Smith at 963-5589)