



**Contact Information:**

**Cyber Criminal Intelligence Program**

**27130 Telegraph Road**

**Quantico, Virginia 22134**

**Phone: 571.305.4485**

**Fax: 571.305.4189**

**E-mail:**

[cybercrimintel.cciu@us.army.mil](mailto:cybercrimintel.cciu@us.army.mil)

**CCIU Web Page:**

[www.cid.army.mil/cciu.html](http://www.cid.army.mil/cciu.html)

**CID Cyber Lookout**  
**On Point for the Army**

**DISTRIBUTION:**

**This document is authorized for wide release with no restrictions.**

2CAN 0025-11-CID361-9H

9 May 2011

## E-MAILS ABOUT BIN LADEN MIGHT PACK A MALICIOUS PUNCH

**OVERVIEW:**

Cyber criminals are wasting no time in capitalizing on the death of Usama bin Laden to obtain personal information from unsuspecting persons or trick them into installing malicious software (malware). Their strategy involves exploiting human curiosity by manipulating unwary users into performing actions that they would not normally take. With the latest headline news regarding the demise of America's most wanted terrorist, malicious e-mail traffic is spreading across the Internet with the help of social engineering attacks that combine tempting e-mail messages with malware.

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

**CURIOSITY SEEKERS BEWARE:**

According to an FBI news release which "warns computer users to exercise caution when they receive e-mails that purport to show photos or videos of Usama bin Laden's recent death. This content could be a virus that could damage your computer."

Experts recommend that computer users never open any unsolicited e-mail or click on any links provided in them.

By following these suggestions, you can help prevent yourself from becoming the next victim:

- ◆ Do NOT trust unsolicited e-mail
- ◆ Employ the use of a spam filter
- ◆ Treat all e-mail attachments with caution
- ◆ Do NOT click links in unsolicited e-mail messages
- ◆ Install antivirus software, and keep its virus signature files up-to-date
- ◆ Turn off the option to automatically download attachments
- ◆ Block executable and unknown file types at the e-mail gateway
- ◆ Configure your e-mail client for security





**PROTECTING YOUR HOME COMPUTER:**

The Army Computer Emergency Response Team offers free antivirus software for Department of the Army personnel to use on home computers. You must access the following link from a .mil computer system and authenticate with your CAC and PIN:

<https://www.acert.1stiocmd.army.mil/Antivirus/>

**ADDITIONAL REPORTING AND INFORMATION:**

US-Cert:

<http://www.us-cert.gov/current/>

Fox News:

<http://www.foxnews.com/scitech/2011/05/04/beware-bin-laden-spam-malware-fbi-warns/>

CNN:

[http://articles.cnn.com/2011-05-04/tech/fake.bin.laden.scam\\_1\\_show-bin-privacy-settings-facebook?s=PM:TECH](http://articles.cnn.com/2011-05-04/tech/fake.bin.laden.scam_1_show-bin-privacy-settings-facebook?s=PM:TECH)



*CCIU is now using the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.*

Disclaimer: The appearance of hyperlinks in this 2CAN, along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this 2CAN.



***CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.***