

2CAN 0011-07-CID221-9H

23 FEBRUARY 2007

## WIRELESS (IN)SECURITY: WHO'S SNOOPING ON YOUR HOME NETWORK?

### OVERVIEW:

A recent article in *The Washington Post* (registration required to view linked article) underscored the dangers of unsecured wireless home networks and access points. Detectives from the Arlington County (Virginia) Police Department served a search warrant at a high-rise apartment, expecting to find a suspected pedophile who had transmitted child pornography online. The detectives were quite surprised to find an elderly woman who had nothing to do with the crime but had an unsecured wireless home network likely used by the real culprit and other Internet surfers in the building. These other individuals could have also captured any data sent and received by the elderly woman over her wireless connection.

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

### AN EMERGING PROBLEM:

Wireless networks, also known as Wi-Fi (Wireless Fidelity), can now be found in almost every public environment, and many individuals have set up wireless at home due to its relatively low cost, ease of installation, and convenience. Unfortunately, many wireless devices fresh out of the box require that the user activate the various layers and methods of security, and establishing an appropriate level of security is not always as easy as getting the wireless set up for use.

As the incident in Arlington highlights, unsecured wireless home networks can be an attractive target for wireless hackers who want to snoop on your activities, steal your data, and surf on your network. According to studies by the computer security firm *Symantec*, almost 50 percent of consumers with home wireless access points are not using encryption to protect their networks. Unencrypted wireless traffic can be "sniffed" from the airwaves by "wardrivers" using freely downloaded software available on the Internet. The Web site <http://www.Wi-Fihotspotlist.com/> even allows you to search for local wireless hotspots, information that can be convenient for hackers and non-hackers alike.

### RECENT HIGH-PROFILE WIRELESS SECURITY INCIDENTS:

- The home improvement company Lowe's learned a lesson about wireless security when three men sitting in a vehicle in a North Carolina Lowe's parking lot compromised the Lowe's wireless network used for transmitting credit card and other data from cashiers to a central network. Not only did these hackers capture credit card information, but they actually altered the software code used by the store to process credit cards and accessed computers in six other Lowe's stores as far away as California. Lowe's did not notify the FBI until they discovered the intrusion at their headquarters. FBI Special Agents on the lookout for suspicious activity found the men in a Lowe's parking lot, followed them home, and arrested them. The men later admitted they had discovered the unprotected network while wardriving. (Source: [FBI Press Release](#))



### Contact Information:

**Cyber Criminal Intelligence Program**  
9805 Lowen Road, Building 193  
Fort Belvoir, Virginia 22060-5598

**Phone: 703.805.3499 (DSN 655)**

**Fax: 703.805.2351 (DSN 655)**

**E-mail:**

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

### CCIU Web Page:

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

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

### DISTRIBUTION:

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



"DO WHAT HAS TO BE DONE"

- In Maryland, an individual began sending harassing e-mails to the president and customers of a competing company and demanded \$17 million in exchange for not releasing proprietary information. The FBI traced the emails to two homes and a dentistry clinic in Arlington, Virginia, and it was discovered that these locations were all running unsecured wireless access points. The suspect was caught, due in part, to his instructions for the extortion checks to be made out in his name. (Source: [\*The 802.11 Technology Gap – Case Studies in Crime\*](#))
- The wireless network of the Wake Internal Medicine Company of Raleigh, North Carolina, experienced a major security breach when an individual accessed 2,000 patient records and sent copies of these records to the affected patients and to several news media outlets. Although security weaknesses had facilitated unauthorized access to the wireless network, auditing and logging software that was in place allowed investigators to uncover identifiable information about the culprit's computer which led to his arrest and conviction. (Source: [\*The 802.11 Technology Gap – Case Studies in Crime\*](#))
- In Toronto, police stopped an individual driving a car the wrong way on a one-way street in a residential neighborhood. Of note was the discovery that the individual was partially clothed and using a laptop computer to download child pornography. Due to unsecured wireless access points in the neighborhood, the individual was able to surf on several open networks. Were it not for his bad sense of direction, the culprit might have continued to use the neighbors' networks for illegal purposes. (Source: [\*The 802.11 Technology Gap – Case Studies in Crime\*](#))

#### **WIRELESS HOME NETWORK SECURITY TIPS:**

- Turn on encryption.
- Change the default service set identifier (SSID).
- Enable the Media Access Control (MAC) address filtering.
- Disable the SSID.
- Do not auto-connect to open/unknown wireless networks.
- Assign static Internet Protocol (IP) addresses to devices.
- Enable firewalls on each computer and router.
- Position the router or access point safely.
- Turn off the network when it's not in use.

#### **ADDITIONAL WIRELESS SECURITY RESOURCES:**

HowStuffWorks.com:

<http://computer.howstuffworks.com/wireless-network.htm>

Free online course from CNET.com:

<http://wireless-basics.classes.cnet.com/lesson-5/>

Wireless Security Initiative from Symantec and GetNetWise:

<http://spotlight.getnetwise.org/wireless/>

White papers from the SANS Institute (Caution - high geek factor):

[http://www.sans.org/reading\\_room/whitepapers/wireless/](http://www.sans.org/reading_room/whitepapers/wireless/)

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.**

# CYBER CRIMINAL INTELLIGENCE PROGRAM CUSTOMER SURVEY

Dear Customer:

Please take a moment and complete this survey to help evaluate the quality and value of CCIU Cyber Criminal Intelligence products. Your response will help us to serve you more effectively and efficiently in the future. Thank you for your assistance.

**Product Title:** \_\_\_\_\_

**Customer's Organization (optional):** \_\_\_\_\_

Marking instructions: Indicate the appropriate response accordingly.

- 1 Strongly Disagree
- 2 Disagree
- 3 Neither Agree nor Disagree
- 4 Agree
- 5 Strongly Agree
- NA Not Applicable

QUALITY						
1	2	3	4	5	NA	
						The product was timely and relevant to your mission, programs, priorities, or initiatives.
						The product was clear and logical in the presentation of information with supported judgments and conclusions.
						The product is reliable (i.e., sources are well-documented and reputable).

VALUE						
1	2	3	4	5	NA	
						The product contributed to satisfying intelligence gaps or predicated cases, especially in previously unknown areas.
						The product resulted in a shift to address previously overlooked investigative areas.
						The product resulted in more informed decisions concerning investigative initiatives and/or resource allocation.
						The product identified new information associated with pending matters or offered insights into information that could change the working premise in a program or initiative.

ADDITIONAL COMMENTS

If you have the free Acrobat Reader, please click below to print your completed survey and mail or fax it to CCIU (address/fax information on front page).

If you have Acrobat Professional, please click below to extract this page, save a copy of the completed survey, and e-mail it to: [cybercrimintel.cciu@us.army.mil](mailto:cybercrimintel.cciu@us.army.mil)