Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cyber Crime Alert Notice

2CAN 0023-07-CID221-9H 12 April 2007

OPSEC on the Cyber Home Front

Overview:

Operations Security (OPSEC) is an all-inclusive term describing efforts to prevent adversaries from acquiring sensitive information. While OPSEC helps the Army maintain superiority over adversaries in peace, crisis, or war, it also offers some valuable lessons for safeguarding families on the Internet. The proliferation of social networking Web sites, Web logs (blogs), chat rooms, and message boards allow Army family members to share information and pictures with friends across the world, but these forums can allow online predators and other criminals to collect and assemble potentially sensitive information.

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

The OPSEC Process - Cyber Home Front Version:

By adapting the Army's OPSEC Process for the cyber home front, Army families can take a risk management approach to how much or how little personal information they make available on the Internet. At one end of the spectrum is a family who has no presence on the Internet, but this might create a feeling of isolation from one's family and friends. At the other end of the spectrum is a family that puts every aspect of their lives on the Internet for the general public to see. The OPSEC Process provides families with mechanisms to assess where they should be on that openness spectrum. A guiding principle is to think like one's adversary: If I were an online predator or criminal, what would I want to know, and how could I collect the information?

- **Identification of critical information** - This step focuses on determining what information needs protection. Although certain information such as property records might be a matter of public record, other personal information should not be readily available to everyone. Again, by thinking like the adversary, parents can identify critical information relating to their families: where children attend school, after-school activities, sports teams, hobbies, birthdays, work schedules, vacation plans, and pictures.

- **Analysis of threats** - This step focuses on learning more about the adversaries' capabilities. There are many online resources for families to educate themselves on the wide spectrum of criminals who use the Internet and the threats they pose.

- **Analysis of vulnerabilities** - Families should conduct a comprehensive assessment of what critical personal information is available on the Internet. Doing a Google search might produce some surprising and alarming results. The vulnerability assessment should also include determining whether children have profiles on social networking Web sites such as MySpace, FaceBook, and Xanga, and if so, how safe the profiles are. Chat rooms represent an additional way for online predators to interact with children, so parents should take note of children's usage.

- **Assessment of risks** - This step involves the risk management calculation: striking an appropriate balance between too much personal information and none at all. Each family has to make an informed decision about what security countermeasures to employ.

- **Application of appropriate countermeasures** - Implementing those steps to eliminate or mitigate identified vulnerabilities.

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

CCIU Web Page:
www.cid.army.mil/cciu.htm

Distribution:
This document is authorized for wide release with no restrictions.

"Do What Has To Be Done"

A Favorite Tactic - Social Engineering:

Social Engineering has been referred to as "people hacking" and essentially involves "the art and science of getting people to comply with your wishes." (Source: *Social Engineering*) Hackers frequently use various forms of Social Engineering as a means to gain access to protected computer systems and obtain personally identifiable and financial information. But Social Engineering also represents a significant OPSEC threat for Army families on the cyber home front.

In a white paper for the SANS Institute, Malcolm Allen describes the Social Engineering cycle as consisting of four distinct phases:

- **Information gathering** - In the context of Internet safety, an adversary can use a variety of resources to build a virtual dossier on the target. Social networking sites, chat rooms, blogs, and Web pages (personal, schools, and clubs) are packed with useful personal information and pictures.

- **Developing relationship** - An adversary uses the collected personal information as a means to establish trust and familiarity with the target. For example, an adversary can initiate contact through e-mail or a chat room and pretend to share the same interests or attend a neighboring school.

- **Exploitation** - An adversary will take advantage of the established relationship to obtain information from the target or persuade the target to perform some task. For online child predators, this task could be meeting in person or providing/accepting explicit pictures or videos.

- **Execution** - The target completes the requested task.

Additional OPSEC and Internet Safety Resources:

McGruff the Crime Dog's "Take a Bite Out of Cyber Crime" initiative:
http://www.bytecrime.org/

National Center for Missing and Exploited Children's NetSmartz411:
http://www.netsmartz411.org/

SGT Firewall On Cyber Patrol (AKO only):
https://www.us.army.mil/suite/page/190357

A cautionary, but fictional tale about OPSEC on the cyber home front:
http://www.snopes.com/horrors/parental/shannon.asp

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.

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: 2CAN 0023-07 - OPSEC on the Cyber Home Front

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 contemporary Internet safety issues.
○	○	○	○	○	○	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 your knowledge of previously unknown Internet safety subjects.
○	○	○	○	○	○	The product caused you to pay more attention to Internet safety subjects relevant to your or your family.
○	○	○	○	○	○	The product increased your familiarity with CID Cyber Lookout's Internet safety initiatives.
○	○	○	○	○	○	The product caused you to research Internet safety subjects in greater depth, using the additional resources listed in the product.

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

PRINT

EXTRACT