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

Cyber Crime Alert Notice

* This archived document may contain broken links.

2CAN 0005-14-CID361-9H 5 February 2014

Unsolicited Software or Devices

Cybercriminals use many techniques to compromise individuals, computers, and entire networks. Cybercriminals are adaptive and innovative and their tactics, techniques, and procedures evolve faster than defenders can keep up with. Therefore, in order to protect vital information and computer systems users must vigilantly consider the implications of unexpected or unusual events and circumstances.

Receiving unsolicited goods, such as software or hardware, is one good example of a situation that should make you cautious. These "gifts" could be from a cybercriminal, who is hoping that you will install them on your personal or government computer so that they will have unfettered access to all the information there.

If you receive unsolicited software or hardware, whether in person, by mail, or package delivery service, you should proceed with an abundance of caution. These items could compromise or corrupt computers and networks. Aside from the obvious problems that would cause, there are regulatory, policy and legal implications to installing, whether knowingly or unwittingly, unauthorized hardware or software on Government systems. Despite this, some users violate these regulations and laws and are subject to criminal or administrative sanctions or even losing their jobs.

The upshot of this is: DO NOT install software or hardware on any Government computer system until properly approved and authorized. If you receive unsolicited goods, contact your supervisory chain of command, security officer, and ethics attorney. You should exercise similar caution with your own electronic systems, which may contain financial, medical, and other highly personal information which could fall prey to the cybercriminal.

Finally, even if the unsolicited software or device isn't from a cybercriminal, it could still present a problem. DoD personnel may not, directly or indirectly, solicit or accept a gift: from a prohibited source or one that is given because of the employee's official position. A prohibited source is a person seeking official action from, doing business with, conducting activities regulated by the employee's employer, or someone who has interests that may be substantially affected by performance or nonperformance of the employee's official duties. Acceptance of a gift worth more than $20 from a prohibited source is prohibited. See 5 USC § 7353, Gifts to Federal employees, and paragraph 2-100 of *DoD 5500.07-R*, Joint Ethics Regulation, or consult your ethics counselor. Remember, however, that even if acceptance of the gift is permitted, using it on government network without the appropriate permission is not and using it on your own computer system could pose dangers similar to the ones set out above.

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

E-mail

CCIU Web Page

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"

The following activities are specifically prohibited by any authorized user on a Government provided computer system or connection:

- Installation of software.
- Modification of the computer system or software, use of it in any manner other than its intended purpose, or adding user–configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications.
- Installation of non-Government-owned computing systems or devices without prior authorization of the Designated Approving Authority (DAA) including but not limited to USB devices, external media, personal or contractor-owned laptops, and mobile computing devices…
- Disabling or removing security or protective software and other mechanisms and their associated logs from the computer system.

Refer to AR 25-2 Information Assurance, 4-5 Minimum information assurance requirements, *(a) Prohibited activities* for a complete list of prohibited activities on Government computer systems.

For more information about computer security and other computer related scams, we encourage readers to visit the CCIU website to review previous cyber crime alert notices and cyber crime prevention flyers.

U.S. Computer Emergency Response Team

- **Cybersecurity for Electronic Devices**
- **Using Caution with USB Drives**
- **Protecting Portable Devices: Physical Security**
- **Protecting Portable Devices: Data Security**

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Disclaimer: The appearance of hyperlinks in this 2CAN, along with the views and opinions of authors, products or services contained therein do 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.

ICE

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

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