

2CAN 0015-12-CID361-9H

24 August 2012



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

CCIU Web Page:

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"

"PHONEY TECH SUPPORT"

OVERVIEW:

The purpose of this Cyber Crime Alert Notice (2CAN) is to inform all service members and Department of the Army civilians of the latest scam wherein cybercriminals are using social engineering techniques to gain access to U.S. Army computer systems. Social engineering is a way for cybercriminals to gain access to your personal information and U.S. Army data. The purpose of social engineering is usually to trick you into handing over your passwords or sensitive data, cause you to unknowingly install malicious software onto your computer, or trick you into purchasing software that your computer does not need. There has been an increase in the number of scams targeting U.S. Army installations, which involves cybercriminals calling people on the telephone, claiming to be from Microsoft Tech Support, and offering to help solve their computer problems. CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

Background:

Social engineering is described as a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking people into breaking their normal security procedures. Social engineering is similar to a confidence trick or simple fraud; the difference is that it is typically used for the purpose of gathering information or gaining access to computer systems. In most cases the attacker never comes face-to-face with the victims.

MICROSOFT Alert:

Microsoft is warning users of the Tech Support Phone Scam, which is designed to trick users into granting the criminal remote access to the user's computer system. The telephone scammers often posed as Microsoft employees from a variety of departments, including Windows Helpdesk, Windows Service Center, Microsoft Tech Support, Windows Technical Department Support Group and Microsoft Research and Development Team. The scammers typically use social engineering skills to convince users into installing programs which are in reality malicious software onto their computer or direct them to websites that would surreptitiously install malicious code that would allow the scammers remote access to the users' computer systems. Many malicious software programs are designed to capture sensitive information or financial data, to include online banking credentials and passwords. If scammers are granted remote access to your computers, they can easily-adjust the settings in a way that could leave your computer easily accessible to future attacks.

"AMMY SCAM" :

In one version of these kinds of scams, the victims were contacted by an individual with a "heavy foreign accent" purporting to be from Microsoft to "fix" their machines. The scammer directed the victims to go to a website where a software program called "Ammy Admin" can be downloaded and installed, which will allow remote access to the victims' computer to allow the supposed

Microsoft employee to fix the problems on the user's computer. In one case, the scammer instructed one of the victims to go a website, designed specifically for granting/gaining remote access, and provided them with a PIN number to enter. Once the victim entered the PIN and started the download, the scammer had complete access to their computer.

HOW NOT BE A VICTIM:

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

- Do NOT trust unsolicited calls
- Do NOT provide any personal information to telephone solicitor
- NEVER give control of your computer to a third party
- Take the caller's information down and immediately report the incident to your local Information Security Officer (ISO).
- HANG UP!

Remember Microsoft or any legitimate company will not make unsolicited telephone calls to help you with your computer problems. If you receive such telephone calls, hang up and notify your ISO for verification. Any technical support on a U.S. Army system should come directly from your ISO and not from a third party.

For more information about computer security and other computer related scams, we encourage Army Knowledge Online users to visit the [On Cyber Patrol Website](#) and review previous 2CANs and other relevant information products. Other users, we recommend that you visit the [CCIU website](#) to review previous 2CANs.

PROTECTING YOUR HOME COMPUTER:

The Army Computer Emergency Response Team (ACERT) 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: To go to the ACERT website [click here](#).

ADDITIONAL REPORTING AND INFORMATION:

U.S. CERT
<http://www.us-cert.gov/alerts-and-tips/>

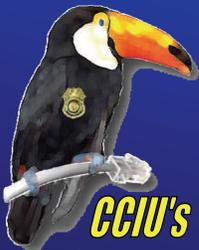
MICROSOFT
<http://www.microsoft.com/security/online-privacy/avoid-phone-scams.aspx>

SYMANTEC
<http://www.symantec.com/connect/blogs/technical-support-phone-scams>



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.