2CAN 0006-07-CID221-9H 31 JANUARY 2007

"VISHING" IS THE NEW "PHISHING"

OVERVIEW:

The Better Business Bureau (BBB) is warning consumers about a new scam that uses Voice over Internet Protocol (VoIP) phones to steal financial information. This technique has been dubbed "vishing" -- short for voice (or VoIP) phishing.

The Federal Trade Commission's OnGuard Online initiative provides practical tips for preventing Internet fraud, and they define phishing as: "A scam where Internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims."

Vishing combines the social engineering aspects of phishing with the relative anonymity afforded by Internet telephony. Some VoIP services allow callers to enter a phone number that will be displayed on the recipient's caller ID. Clever fraudsters will use toll-free prefixes or area codes in the call recipient's general region. When in doubt, individuals should contact their financial institution or other service provider using the phone number on their credit card or billing statement.

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

BBB ARTICLE:

The following article about vishing was posted on the BBB's Web site (http://www.bbb.org/alerts/article.asp?ID=715):

> It can work one of two ways. In the online version, the con artist sends a blast e-mail, disguised to appear as though it's from a financial institution, an online payment service such as PayPal or other well-known business. The e-mail which may have a trusted logo, typically reports a "security" problem with the recipient's account and urges the victim to call a telephone number to "straighten things out."
>
> The recipient, who knows better than to click on imbedded hyperlinks in strange e-mails for fear of being "phished," feels safer calling a telephone number.
>
> The area code might be a local one they easily recognize or appear to be toll-free. When the victim calls, they reach an automated attendant prompting them to enter their account number, password or other private information for "security verification" purposes.
>
> Some "vishers" use automated dialing programs to "cold call" victims. The caller ID device may list a legitimate-looking local phone number, to inspire trust from the recipient. A prerecorded message (or sometimes a live "employee") claims the victim's account has been compromised or needs updating or verification. The victim is asked to enter their account information, which is digitally transcribed onto the hard drive of the scammer's computer for later retrieval.

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

CID Cyber Lookout
On Point for the Army

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

The BBB offers consumers these tips to protect against "vishing" scams:

- Typical "vishing" e-mails imply urgency, ask you to verify account information, and may contain misspellings.
- If you receive a "vishing" phone call, hang up. Call your bank, using the phone number on the back of your debit or credit card, and report the matter.
- Banks do not use prerecorded messages to handle security issues. If they telephone you to report suspicious use of your card, they do not need to request identifying information because they already have that on record.
- Do not automatically trust a phone number based on its area code. Con artists can hack into Caller ID systems, and VoIP users can assign any area code to a phone number.

If you think you have been a victim of "vishing" visit the Federal Trade Commission's Identity Theft Web site at www.consumer.gov/idtheft/con_about.htm.

ADDITIONAL REPORTING AND INFORMATION ABOUT VISHING:

vnunet.com:
http://www.vnunet.com/vnunet/news/2160004/cyber-criminals-talk-voip

USA Today:
http://www.usatoday.com/tech/news/internetprivacy/2006-07-12-vishing-scam_x.htm

PC Magazine:
http://www.pcmag.com/article2/0,1895,1981797,00.asp

CIO.com:
http://www.cio.com/archive/090106/tl_vishing.html

ADDITIONAL IDENTITY THEFT RESOURCES:

Federal Trade Commission's OnGuard Online:
http://onguardonline.gov/index.html

International Association of Chiefs of Police ID Safety:
http://www.idsafety.org/

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 0006-07 - "Vishing" is the New "Phishing"

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 predicating 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).

PRINT

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

EXTRACT