

SUBJECT: ALARACT 166/2008
TEXT:
UNCLASSIFIED//

THIS MESSAGE HAS BEEN SENT BY THE PENTAGON TELECOMMUNICATIONS CENTER ON BEHALF OF DA WASHINGTON DC//DAMO-AOC//G-3 SENDS//

PASS TO ALL SOLDIERS, DA CIVILIANS, AND SUPPORTING CONTRACTORS.

REF/A/ARMY REGULATION 530-1//19 APRIL 2007//DEPARTMENT OF THE ARMY OPERATIONS SECURITY (OPSEC) (FOUO): THIS REGULATION IS APPLICABLE TO MILITARY AND CIVILIAN PERSONNEL OF THE ACTIVE ARMY, ARMY NATIONAL GUARD OF THE UNITED STATES, AND THE UNITED STATES ARMY RESERVE, AND RELATED ACTIVITIES OF THOSE ORGANIZATIONS.

REF/B/FEDERAL BUREAU OF INVESTIGATION, CYBER CRIME SECTION, INTERNET CRIME COMPLAINT CENTER, INTELLIGENCE BULLETIN//
4 MARCH 2005: PHARMING - NEW METHOD OF IDENTITY THEFT.

REF/C/ONGUARD ONLINE.GOV/PHISHING - ONGUARDONLINE.GOV PROVIDES PRACTICAL TIPS FROM THE FEDERAL GOVERNMENT AND TECHNOLOGY INDUSTRY TO HELP GUARD AGAINST INTERNET FRAUD, SECURE COMPUTERS, AND PROTECT PERSONAL INFORMATION.

SUBJECT: ONTAP 08-02 - OPSEC: PREVENTING IDENTITY THEFT

1. THE ARMY CASUALTY AND MORTUARY AFFAIRS OPERATIONS CENTER (CMAOC) REPORTED A RECENT PHISHING SCAM CONCERNING FAMILIES OF DECEASED SOLDIERS. THE SCAM PURPORTS TO BE FROM DEFENSE FINANCE AND ACCOUNTING SERVICE (DFAS) AND ARMY HUMAN RESOURCES COMMAND (HRC) AND INFORMS FAMILIES OF DECEASED SOLDIERS THAT THEY ARE ENTITLED TO MONETARY COMPENSATION IN EXCESS OF \$12,000,000 THAT WILL BE AVAILABLE TO THEM IN ONE WEEK IN EXCHANGE FOR PERSONALLY IDENTIFIABLE INFORMATION (PII) SUCH AS SOCIAL SECURITY NUMBERS, DATES OF BIRTH, ADDRESS, ETC. THEN, THEY ARE ADVISED TO EMAIL THE PII TO AN OVERSEAS YAHOO ACCOUNT TO EXPEDITE PAYMENTS.

2. A PHISHING ATTACK IS A FORM OF SOCIAL ENGINEERING USED BY IDENTITY THIEVES (CRIMINALS) TO COLLECT PII WHICH THEY USE TO COMMIT FRAUDULENT ACTIVITY. SOCIAL ENGINEERING SCHEMES USE SPOOFED EMAILS TO LEAD INDIVIDUALS TO WEBSITES THAT APPEAR TO BELONG TO A LEGITIMATE BUSINESS. ONCE ON THE WEBSITE VISITORS ARE ASKED TO PROVIDE FINANCIAL DATA SUCH AS CREDIT CARD NUMBERS, ACCOUNT USERNAMES, PASSWORDS, ETC.

3. ACCORDING TO THE FEDERAL BUREAU OF INVESTIGATION (REF 2) PHARMING IS A MALICIOUS WEB REDIRECT AND IS IMPLEMENTED WHEN AN INDIVIDUAL, TRYING TO REACH A LEGITIMATE SITE, IS UNKNOWINGLY SENT TO A FRAUDULENT SITE. THIS ALLOWS THE PHARMER TO OBTAIN SENSITIVE PII FOR THE FURTHERANCE OF CRIMINAL ACTIVITIES. A REDIRECT IS CONDUCTED BY USING TROJANS, WORMS, AND OTHER TECHNOLOGY WHICH ATTACKS THE BROWSER ADDRESS BAR. ANOTHER METHOD IS USED BY ATTACKING THE DOMAIN NAME SERVICE (DNS) SYSTEM. BY DOING SO, EVERYONE WHO ENTERS A VALID UNIFORM RESOURCE LOCATOR (URL) (COMMONLY REFERRED TO AS A LINK) WILL BE REDIRECTED TO A FRAUDULENT SITE. THE DNS IS A SERIES OF DOMAIN SERVERS WHICH ARE LARGE DIRECTORIES OF COMMON NAMES (SUCH AS GOOGLE AND AMAZON) THAT LOCATE THE ACTUAL REGISTERED INTERNET ADDRESS A USER IS SEARCHING FOR.

4. ALL ARMY PERSONNEL, TO INCLUDE DA CIVILIANS AND SUPPORT CONTRACTORS SHOULD TAKE PRECAUTIONS TO PREVENT THEMSELVES FROM BECOMING VICTIMS OF PHISHING, PHARMING, AND OTHER TYPES OF INTERNET SCAMS. ARMY PERSONNEL SHOULD ALSO INFORM FAMILY MEMBERS ABOUT SCAMS AND URGE THEM TO TAKE PRECAUTIONARY MEASURES WHEN USING THE INTERNET.

5. THE FOLLOWING MAY BE INDICATORS OF A SCAM:

A. SUSPICIOUS EMAIL ADDRESS
B. GENERIC SUBJECT LINE AND MESSAGE BODY
C. POOR USE OF ENGLISH
D. SUSPICIOUS HYPERLINKS
E. SUSPICIOUS ATTACHMENTS
F. ATTACHMENTS CONTAINING MACROS (YOU MAY BE ASKED TO ENABLE MACROS)
G. REQUESTS FOR PII (SUCH AS SSN, DOB, PASSWORDS, ETC.)

6. TO AVOID VICTIMIZATION, THE FOLLOWING PRECAUTIONS ARE ADVISED FOR USE ON PERSONAL COMPUTERS:

A. DO NOT REPLY TO EMAIL OR POP-UP MESSAGES FROM SUSPICIOUS OR UNTRUSTED SOURCES THAT ASK FOR PERSONAL OR FINANCIAL INFORMATION, AND DO NOT CLICK ON LINKS IN THE MESSAGE. DO NOT CUT AND PASTE A LINK FROM A MESSAGE INTO YOUR WEB BROWSER - PHISHERS CAN MAKE LINKS LOOK LIKE THEY GO TO A CERTAIN PLACE, BUT THEY ACTUALLY SEND YOU TO A DIFFERENT SITE. SIMPLY DELETE THE SUSPICIOUS EMAILS.

B. SOME SCAMMERS SEND AN EMAIL THAT APPEARS TO BE FROM A LEGITIMATE BUSINESS AND ASK YOU TO CALL A PHONE NUMBER TO UPDATE YOUR ACCOUNT OR ACCESS A REFUND. BECAUSE THEY USE VOICE OVER INTERNET PROTOCOL TECHNOLOGY, THE AREA CODE YOU CALL DOES NOT REFLECT WHERE THE SCAMMERS REALLY ARE. IF YOU NEED TO REACH AN ORGANIZATION YOU CONDUCT BUSINESS WITH, CALL THE NUMBER ON YOUR FINANCIAL STATEMENTS OR ON THE BACK OF YOUR CREDIT CARD.

C. USE ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE, AS WELL AS A FIREWALL, AND UPDATE THEM REGULARLY.

D. DO NOT EMAIL PERSONAL OR FINANCIAL INFORMATION.

E. REVIEW CREDIT CARD AND BANK ACCOUNT STATEMENTS AS SOON AS YOU RECEIVE THEM TO CHECK FOR UNAUTHORIZED CHARGES.

F. BE CAUTIOUS ABOUT OPENING ANY ATTACHMENT OR DOWNLOADING ANY FILES FROM EMAILS YOU RECEIVE, REGARDLESS OF WHO SENT THEM.

G. FORWARD PHISHING EMAILS TO SPAM@UCE.GOV - AND TO THE COMPANY, BANK, OR ORGANIZATION IMPERSONATED IN THE PHISHING EMAIL. YOU ALSO MAY REPORT PHISHING EMAIL TO REPORTPHISHING@ANTIPHISHING.ORG. THE ANTI-PHISHING WORKING GROUP, A CONSORTIUM OF ISPS, SECURITY VENDORS, FINANCIAL INSTITUTIONS AND LAW ENFORCEMENT AGENCIES, USES THESE REPORTS TO FIGHT PHISHING.

7. IF YOU HAVE BEEN THE VICTIM OF AN INTERNET SCAM, VISIT THE FEDERAL TRADE COMMISSIONS IDENTITY THEFT WEBSITE AT FTC.GOV/IDTHEFT FOR RECOVERY GUIDANCE.

8. IF A PHISHING, PHARMING, OR OTHER NETWORK SCAM IS SUSPECTED ON A GOVERNMENT COMPUTER OR NETWORK, FOLLOW LOCAL COMMAND INFORMATION ASSURANCE (IA) RESPONSE AND REPORTING PROCEDURES.

9. THE ARMY COMPUTER EMERGENCY RESPONSE TEAM - COMPUTER NETWORK OPERATIONS (ACERT-CNO) IS THE OFFICIAL US ARMY LOCATION FOR ANTIVIRUS PRODUCTS, DOCUMENTATION, AND DEFINITION UPDATES. THE ACERT-CNO PROVIDES ANTIVIRUS UPDATES, FREE OF CHARGE, TO GOVERNMENT EMPLOYEES. FOR MORE INFORMATION, VISIT THE FOLLOWING AKO WEBPAGE: WWW.US.ARMY.MIL; SELECT SELF-SERVICE; SELECT ANTIVIRUS SERVICES. THE PAGE EXPLAINS ENTITLEMENTS AND PROVIDES DOWNLOADS.

10. THE ARMY G-3/5/7 POC FOR THIS ONTAP IS THE ARMY OPSEC PROGRAM MANAGER, COL WESLEY MARTIN, DAMO-ODI. EMAIL QUESTIONS OR CONCERNS TO CPT CLEMENT DANISH, AT CLEMENT.DANISH@HQDA.ARMY.SMIL.MIL, OR CONTACT MS ANGELA SYKES, AT DSN: 224-6558, COMM: 703-614-6558.

11. THE EXPIRATION DATE OF THIS MESSAGE CANNOT BE DETERMINED.