



United States Army Criminal Investigation Command

Media contact: CID Public Affairs Office
571-305-4041

FOR IMMEDIATE RELEASE

CID Lookout On Point for the Army

CID Warns of Government Travel Card Phishing Scam

QUANTICO, Virginia, January 23, 2014 – The U.S. Army Criminal Investigation Command, commonly referred to as CID, is warning the greater Army community about a new phishing scam where criminals are targeting U.S. Government Travel Card holders.

Over the last few days, Citi, the Government Travel Charge Card provider, has received calls informing them of a new phishing scam where cardholders have reported receiving suspicious text messages from 19014140142@VTEXT.COM.

The false text messages state that the cardholder's account will be suspended unless certain information is verified such as the full account number, the Card Verification Value (CVV) number on the back of the card, the last four digits of the cardholder's social security number, and the four-digit PIN.

This text message **is not a legitimate or official message** and cardholders are advised not to respond to the request for information.

As a precaution, the suspicious phone number where the text messages originated from has been disconnected by the Federal Trade Commission (FTC) and now has a pre-recorded message informing callers that they may have been involved in a phishing attack.

The message also informs callers about the specific type of scam that was employed, what steps to take to see if their account has been compromised, and how to prevent becoming a potential victim.

Additional information regarding phishing and other internet scams, as well as general online safety information can be found at www.onguardonline.gov.

-more-

2-2-2
Internet

If you are a **victim** of a phishing scam, the following actions should be completed as soon as possible to assist law enforcement:

- **Report the crime to the Internet Crime Complaint Center (IC3) (FBI-NW3C Partnership)**

Online: <http://www.ic3.gov/default.aspx>

- **Report the crime to the Federal Trade Commission (FTC):**

Online: <http://www.ftc.gov/idtheft>

By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

CID strongly recommends that Soldiers, civilians and family members who have information of any known crime committed by a Soldier or a crime that occurred on their respective post, camp or station to report the incident to their local CID office or email CID at Army.CID.Crime.Tips@mail.mil.

-30-

CID Lookout is a U.S. Army Criminal Investigation Command (USACIDC) initiative to partner with the Army community by providing a conduit for members of the Army family, to help prevent, reduce, and report felony-level crime.

The USACIDC, commonly known as CID, is an independent criminal investigative organization that investigates serious, felony-level crime such as murder, rape, sexual assault, robbery, arson, fraud, and even cyber crime or intrusions into the Army networks (see CID Cyber Lookout).

Solving and preventing these types of crime cannot be achieved solely by CID Special Agents and the Military Police. Together, professional law enforcement officers and the Army community must work hand-in-hand to fight serious crime. As such, CID is *On Point for the Army* and depends heavily on Soldiers, family members and civilian employees to *Be On The Lookout* and provide assistance in keeping the *Army Strong* and safe.

CID Lookout provides the latest information to the Army community aimed at helping Soldiers protect themselves, their families and to reduce their chances of becoming crime victims.

For more information on CID or to report a felony-level crime or provide information concerning a crime, contact your local CID Office or the Military Police, or visit www.cid.army.mil.