

Threatening Email: CID Warns of Old Phishing Scam with New Twist

By CID Public Affairs Office



FORT BELVOIR, Va., February 17, 2009 – The U.S. Army Criminal Investigation Command, commonly known as CID, is warning the greater Army community of an older internet phishing scam with a new twist. CID wants to make the public aware of how to recognize this scam and what actions to take should someone receive it.

According to the FBI, the "Death Roll Squad" phishing scam originated overseas and has been circulating on the internet for more than five years. These scammers can mask their identities and locations allowing them to strike quickly and then disappear leaving little to no trace behind. The scammers attempt to deceive recipients into revealing personal, banking or financial information.

Much like other foreign email scams, the "DRS" scam preys upon the e-mail recipients' emotions. This latest version claims to have personal knowledge of and access to the victims, but the new scheme threatens physical violence if victims do not comply with the e-mail's demands.

Prior e-mail scams, rather than threatening harm to the recipients, appealed to the recipients' sense of empathy or desire for financial gain. By doing what was asked of them in the e-mails, often cashing a check, the recipients were told they would be helping the sender or the sender's family out of a terrible situation in their country. Other scam e-mails promised the victims that if they cashed a check sent to them, they could keep a percentage. These checks were bogus, and the victims were out hundreds or thousands, of dollars.

As fewer people fall victim to these scams, new emails schemes are created. Now with the general public having a better understanding

of what scams are out on the internet, these cyber crooks have moved on to yet another human emotion - fear.

The majority of these scams are mass e-mails, by which no one person is individually targeted, but rather hundreds of thousands of e-mails are blindly sent out. They are usually written in such a way that a person receiving one may think that it was addressed specifically to them.

CID has no reports of the scammers acting on the threats and strongly recommends that Soldiers, civilians and family members who receive any suspicious and/or unsolicited emails should delete them without response. However, if someone receives a threat that they feel is legitimate or has any credibility what so ever, they should immediately contact law enforcement officials.

The United States Secret Service (www.secretservice.gov) and the United States Postal Service (<http://postalinspectors.uspis.gov/>) are the primary U.S. law enforcement agencies dealing with these types of scams. U.S. citizens or residents who have not suffered a financial loss and want to report a scam may forward unsolicited emails to the USSS at 419.fcd@uss.treas.gov. People can also file complaints with the Internet Crime Complaint Center (IC3) at www.ic3.gov/crimeschemes.aspx#item-13

U.S. citizens and residents who have suffered a financial loss should contact the nearest field office of the Secret Service by telephone. Victims are advised to continue reporting these scam e-mails to law enforcement agencies.