U.S. Army Information Technology Agency (ITA)

Strategic Communication Message, November 15, 2010, ITA, Pentagon, Washington, DC

ITA Enterprise Security Services - Pentagon
Information Assurance Division
Information Assurance Awareness Monthly Bulletin

Phishing Scam Targets Military Families

ITA is pleased to provide this information update as part of our commitment to support your information assurance efforts. The theme for this month's bulletin as we approach the holidays is to keep our families and loved ones informed and safe from identity theft and to alert you of a phishing scam that has recently been making the rounds.

A new phishing scam targeting members of the U.S. military and their families was discovered recently. This scam arrives in the form of unsolicited emails purportedly from USAA, which is one of the nation's largest financial services and insurance companies. USAA serves over seven million members and provides banking, investments, and insurance services for current and former military members and their families.

The email usually arrives with the subject titles 'USAA Notification' or 'Urgent Message for USAA Customer'. It contains a link embedded in the email body and attempts to trick people into divulging their personal information such as usernames and passwords to hackers who will then use this information to steal the user's identity.

Those who click on this link will be navigated to a fake login page that looks very similar to the USAA's legitimate website where they are prompted for their personal information. This scam is considered to be quite a sophisticated phishing attack because of the number of different counterfeit USAA websites that have been created to serve this phishing scam.

Here are some ways in which you can protect yourself from falling prey to such a scam. Phishing attempts are usually characterized by a generic greeting and a false sense of urgency. Prior to clicking on any web link within a message or opening up an attachment, confirm the validity of the email source and verify that it is digitally signed. When sending out emails always digitally sign your e-mails. Especially make sure that you digitally sign and encrypt all messages that contain sensitive information. Do not send email using HTML formatting; use Plain Text whenever possible.

To have a better understanding of the threat of phishing, review the Department of Defense Phishing Awareness training available at: http://iase.disa.mil/eta/phishing/Phishing/launchPage.htm
ESS-P delivers monthly information assurance awareness updates as a customer service from ITA.

Respectfully,
ITA Information Assurance
NIPR: ITAIA@conus.army.mil; SIPR: ITAIA@hqda-s.army.smil.mil

Reference: AR 25-2, Para. 2-8(g)
Classification: UNCLASSIFIED
Caveats: NONE

Creating Connections