ITA Enterprise Security Services - Pentagon
Information Assurance Division
Information Assurance Awareness Bulletin
17 December 2010

WikiLeaks and Phishing Scams Associated with Current Events in the Media

ITA is pleased to provide this information update as part of our commitment to support your information assurance efforts. All users are strongly advised against attempting to access information posted on the Internet or browse websites that claim to contain classified information from government owned computing systems. This message is in accordance with Headquarters Department of the Army issued All Army Activities (ALARACT) message issued on August 14, 2010 related to the WikiLeaks website. In addition, the Office of the Administrative Assistant (OAA) Communications has advised that all Department of Defense employees are not permitted to access, review, or search for any material pertaining to the WikiLeaks website from a government-issued computer. **Users are advised that doing so may include the user as part of the formal ongoing investigation.**

With the recent developments and renewed interest in the WikiLeaks articles in the media, there have been reports of phishing scams related to this topic. Unsuspecting users are subject to attacks from hackers who make use of subject lines with topics that are of high interest to the public to send phishing emails. These email messages appear to originate from a valid sender.

All users need to exercise caution when dealing with email messages that have subject lines, attachments or hyperlinks related to the WikiLeaks. The United States Computer Emergency Readiness Team (US-CERT) reminds users to remain vigilant for potential malicious cyber activity seeking to capitalize on interest in this subject matter. Users are advised to exercise caution in handling any email with subject line, attachments, or hyperlinks related to WikiLeaks, even if it appears to originate from a trusted source.

If you observe any of these incidents, it is your responsibility to report it to your System Administrator (SA), Information Assurance Manager (IAM), or the Information Assurance Security Officer (IASO). If you do not have access to any of these personnel at the time of the incident, contact the Pentagon Computer Incident Response Team (PENTCIRT) at pentcirtincid@hqda.army.mil or call 703-695-CIRT (2478).

How can you protect yourself from Phishing Scams?
Do not follow unsolicited web links in email messages. Use caution when opening email attachments. Maintain up-to-date antivirus software. Learn to recognize email scams and understand how social engineering and phishing attacks operate. To learn more information on how to protect yourself from phishing scams, visit the US-CERT at http://www.us-cert.gov/cas/tips/

ITA ESS-P regularly delivers information assurance awareness updates as a service to our customers.
Respectfully,
ITA Information Assurance
NIPR: ITAIA@conus.army.mil; SIPR: ITAIA@hqda-s.army.smil.mil
ITA's website: http://ita.army.mil
Reference: AR 25-2, Para. 2-8(g)
Classification: UNCLASSIFIED
Caveats: NONE