NAVAL POSTGRADUATE SCHOOL
ITACS
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES

TECHNOLOGY NEWS SEPTEMBER 2010

CYBERSECURITY AWARENESS MONTH

During the inaugural year of Cybersecurity Awareness month, in October 2009 ITACS highlighted cybersecurity research at NPS and developed and delivered a number of trainings and events for the community. During Cybersecurity Awareness Month 2010, ITACS will be focusing on the user, not only showing what good cybersecurity practices to use, but how to use them.

ITACS blocks nearly 80% of all incoming e-mail using a spam filter, but the amount of spam is increasing exponentially. Although it has become routine that users receive e-mails that request their NPS computer account credentials, some e-mail can have malicious intent: to steal user credentials, and/or their personal financial information and identity. ITACS' anti-malware protocols are aggressive and sophisticated; however, these attacks require ongoing monitoring and vigilance, and a reinvigoration of awareness trainings to ensure our entire campus community is engaged in protecting our individual and institutional resources. To help in that effort, ITACS will be offering a number of focused classes to small audiences throughout the month. The topics will include:

- Malware and Phishing: How to recognize, respond, be reactive and preventive in regards to phishing and virus activity;
- Privacy: How to protect your information on social networking sites such as Facebook, LinkedIn, and MySpace;
- Passwords: How to create and manage good passwords;
- Signing and Encrypting: How to digitally sign and encrypt your e-mails and recognize them when sent from others.

Additionally, brown bag sessions covering topics such as about Cybercrime, Securing Stored Data, Identity Protection and Quantum Security will be offered by NPS faculty.

Dates and details for Cybersecurity Awareness month events will be posted for the campus on the Intranet; in the interim, here are some useful cybersecurity tips:

- If you don't know the sender, suspect the message isn't authentic, or the e-mail did not come from a NPS user, don't use links in an e-mail.
- Regularly check your bank and credit card statements to ensure that all transactions are legitimate.
- Do not respond to e-mails from any source requesting account names, passwords or personal information. Neither ITACS nor any legitimate business will ask for this information.

Following the example of other universities, ITACS has created a mailbox for suspicious e-mail. If you receive a suspicious e-mail, do not open and/or click on any of its links; rather, create a new e-mail, drag the suspicious e-mail into the new e-mail and send it to NPS Abuse or abuse@nps.edu. If you require any assistance, please contact the Technology Assistance Center at Ext. 1046.

ITACS looks forward to working with the campus gathering more momentum in keeping NPS networks secure.

SPEARPHISHING: STAY INFORMED AND ALERT

Phishing continues to be a matter of concern at NPS because it continues to be the most common technique used by our adversaries to gain unauthorized access to NPS data and networks. In September, NPS experienced a spear-phishing incident in which 18 people were sent a targeted e-mail which contained malicious code. The sender was falsely presented as a senior leader on campus, and the content of the e-mail contained NPS-relevant material. Although the issue was resolved, evaluation is underway on how the spear-phishing incident occurred, particularly because of the serious consequences that could have ensued had the attack been successful.

Another layer of ITACS' defense-in-depth strategy is the installation of a Network Access Control appliance – Safe-Connect – by Impulse Point, which will proactively monitor end-user systems and provide a layer of protection between the network firewall and the Internet by enforcing compliance with antivirus software, virus definitions, and operating system patching preferences on NPS wired, wireless, and home (when connected to the NPS network) computer systems. Safe-Connect is used by higher education institutions such as UCLA, the University of Cincinnati, Denver, Missouri, Nebraska, and Auburn.

Implementation requires a one-time authentication, unauthorized device prevention, verification of antivirus software and definitions, and verification of operating system update preferences. ITACS will be testing the system from July 19th through October 12, 2010; full deployment is scheduled on October 13, 2010.

PARTNERSHIPS AND OUTREACH

During a recent visit to Washington D.C., **Mr. Joe LoPiccolo** had the opportunity to meet with **former Department of Navy CIO and current Deputy Department of Defense CIO Dave Wennergren.** Mr. LoPiccolo briefed Mr. Wennergren on the Schools' efforts on Kuali, the development of the LifeRay portal, ITACS' use of open source solutions — which the Department of Defense (DoD) is starting to adopt — the FAOweb, Sakai Collaborative Learning Environment implementation, Team Monterey efforts, the School's collaborations with other DoD institutions, and the potential ERN initiative with Defense Language Institute.

Mr. LoPiccolo presented IT information materials and the IT Strategic Plan to Mr. Wennergren, a model that Mr. Wennergren is going to use for the development of his area's new strategic plan.

Mr. Wennergren offered his endorsement of NPS, and welcomed further updates on ITACS' efforts.

ITACS will undergo an external review from November 18-19, 2010 by **University of California Santa Cruz Vice Chancellor for IT/CIO Mary Doyle** and **California Institute of Technology CIO John Dundas.**

General Keith Alexander, Director of the National Security Agency, and Commander of the US Cyber Command, was briefed on the Monterey Peninsula Department of Defense Net and the DLI MOU by Dr. Haska during his visit to the campus on September 24.

The **Committee on the Future**, charged by President Oliver to develop a report that will form the basis for the next NPS strategic plan, held its first meeting on August 11, 2010. Chaired by RADM Jerry Ellis, the committee created sub working groups, one of which is Information Technology. Dr. Christine Haska is leading that group in the development of its first status report, which was submitted to RADM Ellis in late September. The IT Task Force will serve in an advisory capacity to this effort

TECHNOLOGY ASSISTANCE CENTER

From September 1 through September 29, 2010, the Technology Assistance Center (TAC) received 4,976 requests for assistance, 4,176 of which were resolved by the Tier 1/Tier 2 areas. The remaining 797 requests were escalated to groups outside of TAC for specialized assistance. This number represents a 48% increase in requests for assistance from September 2009.

Requests for assistance were categorized as follows:

Phone: 2,944
E-Mail: 1,666
Walk-in: 334
Web: 1
Technician: 31

This month, 93% of all calls were resolved within the Service Level Agreement (SLA). Those that were carried over are awaiting parts, pending information from the customers, etc.