Tips for using public wireless works

By Paul Long, CFAY Public Affairs

Naval Criminal Investigative Service (NCIS) has practical tips that may help you protect yourself while surfing the Internet on public wireless networks.

Special Agent Anthony Britt, of Yokosuka's NCIS office says that internet users away from home should use secure hotspots.

"You can be confident a hotspot is secure only if you're asked to provide a Wi-Fi Protected Access (WPA), a type of encryption), WPA2 is the most secure. If you're not sure, the information you enter could be at risk," Britt said.

Public wireless networks – those Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places – allow people to access the internet through a shared network.

"While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information," said Britt.

To determine whther or not a website is encrypted, look for https at the beginning of the web address (the "s" is for secure), and a lock icon at the top or bottom of your browser window.

"Look for https and the lock icon the entire time you're on the site, not just when you sign in," said Britt. "You can also click on the lock icon to display information about the site and help you verify that it's not a fraudulent website."

According to Britt since most Wi-Fi hotspots don't encrypt the information you send over the internet, they are not secure.

"If you use an unsecured network to log in to an unencrypted site – or a site that uses encryption only on the sign-in page – other users on the network can see what you see and what you send," he said.

Also, according to Britt an unscrupulous person could hijack your session and log in as you.

"New hacking tools that are available for free online make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs," he said.

According to Britt, an imposter could use your account to impersonate you and scam people you care about. "An attacker could test your username and password to try to gain access to other websites – including sites that store your financial information," he said.

AE2 (AW) Brad Bumpus, of the *USS George Washington* (CVN 73), surfs the web using MWR's Free HotSpot at the Fleet Recreation Center. NCIS warns internet users to guard against their personal information being stolen online and that all free hotspots aren't secure.

Special Agent Britt has a few suggestions for using a Wi-Fi hot spot. "Only log in or send personal information to websites that you know are fully encrypted. And keep in mind that your entire visit to each site should be encrypted – from the time you log in to the site until you log out," he said. "If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away."

Britt advises that you don't stay permanently signed in to accounts, to create a unique password for every site that you log onto, and if possible, use a virtual private network (VPN). "VPNs encrypt traffic between your computer and the internet, even on unsecured networks," he said.

Britt said some Wi-Fi networks use encryption with Wired Equivalent Privacy (WEP) and WPA; WPA encryption protects your information against common hacking programs. However, WEP may not.

"If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network," he said.

Britt suggests for users to install browser add-ons or plug-ins. "For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites. Be sure look for https in the URL and the lock icon to know a site is secure."

NAVFAC Far East volunteers donate to disaster victims

From NAVFAC Far East Public Affairs

Soon after unprecedented natural disasters and a nuclear crisis struck Japan in March, a group of volunteers at NAVFAC Far East turned a canceled annual celebration into a way to help the Japanese people.

This year's Kanto Plain Seabee Ball, scheduled for April 2, was to celebrate the 69th anniversary of the Seabees, the 144th anniversary of the Civil Engineer Corps and the 169th anniversary of Naval Facilities Engineering Command. It was canceled immediately following the events of March 11 when priorities shifted to relief and recovery efforts.

According to Seabee Ball Committee member, Lt. j.g. Michael Bozek, volunteers opted to buy the unused commemorative coins which had been created for the occasion and donate their money to the American Red Cross's Japan Tsunami Relief fund.

When others learned of this the coins quickly sold out, raising more than $1,200.

"The unselfish actions of our volunteers lived up to the proud Seabee motto," said NAVFAC Far East Executive Officer Capt. Christopher J. Lacaria. "With compassion for others, we build, we fight, for peace with freedom."