



Emergency Cell Phone Usage

Submitted by Stanley J Cantilina
SO-CM DIV 10 01SR

The * CG that was used on the cell phone service to contact the USCG in an emergency has been discontinued. From now on, if only a cell phone is available the boater should dial 911. It should be stressed in the Boating Safety Classes that a VHF Marine Radio is the best way to contact the USCG in an emergency and that the Rescue 21 system only works on the VHF Marine Radio

PHP

Hypertext Preprocessor (PHP) is now operational for all websites hosted on the National Auxiliary Sever. We are running version 4.4.5.

Email Etiquette

Submitted by Darren Lewis – DVC-IP

I'd like to once again plead with everyone to stop forwarding jokes, photos, funny stories, attack warnings, chain letters, and such.

The bad guys are creating attacks that look like valid forwarded messages from friends even down to your name in the message and a nice little note. In some cases opening the message while not even touching an attachment can lead to your computer becoming infected with a virus, worm or trojan. In many cases these attacks are evolving far faster than we, as individuals, can hope to keep up.

We all have a role to play in keeping the internet safe, fun and an effective way to communicate.

- If it is a really good joke, a touching story, or a great poem make a phone call to tell it – It's nice to hear a friends voice.
- If it is a photo you've just got to see either print it and mail the photo or send a URL from a legitimate source to the image.
- Don't forward friends names to dozens of others to serve as spam bait. Recognize that the common e-mail chain petition is not recognized as legitimate by most legislators and regulatory bodies.
- Please don't send chain letters.
- If a message about some new computer vulnerability Write an email and tell where and how to find the solution but check the veracity of the threat first and don't just forward a potentially bogus or uninformed warning.
- Take extreme caution when opening messages sent and keep anti-virus software up to date so that the spammers cannot exploit your machine to send spam or harvest your address book to get contact information.
- Never forward any message without a personalized note as to why it is important and what action to take.

- Avoid forwarding attachments whenever possible and don't forward frivolous attachments. If you do send an attachment it will have passed an anti-virus screening and will be accompanied by an explanatory note.
- Take the Boulder Pledge (http://en.wikipedia.org/wiki/Boulder_Pledge) and don't buy from spammers, ever!

I ask that you consider adopting these guidelines when communicating with your business contacts, Coast Guard/Auxiliary friends and family.

While these steps will not ensure we will not fall victim to internet crime I hope that they will reduce our exposure.

Vista Upgrade vs. Clean Install

Since Vista has come out there seems to be a lot of confusion on what product to purchase and whether a clean install or upgrade is needed. More information can be found at:

<http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/upgradepaths.msp>

AUXDATA and Popup Windows

Adapted from a submission by Robert Fiedler

AUXDATA uses popup windows. Many times we find that problems members are having accessing AUXDATA is that they don't allow pop ups when entering the AUXDATA system. Pop up windows must be allowed in your Internet browser for AUXDATA to function properly. There are various browsers in use so if you are unsure of how to enable pop ups consult the browser documentation. More information on pop up windows can be found at:

Internet Explorer: <http://support.microsoft.com/kb/843016>

Firefox: <http://www.mozilla.org/support/firefox/options>

Safari: <http://www.apple.com/support/mac101/work/20/>

Phishing or Spoofing

Submitted by Jerry Turley, BC-IWA

What is Phishing or Spoofing? -- "Phishing" or "Spoofing" emails are made to look like they are sent from reputable companies but are actually sent by cyber-criminals. These types of emails are sent to trick consumers into divulging sensitive information so that unlawful charges can be made on the consumers' accounts. Responding to "phishing" or "spoofing" emails will put your accounts and personal information at risk; they will link you to an imitation copy of a legitimate web page to trick you into providing sensitive personal information including passwords.

Identifying a Phish or Spoof Email -- Phishing emails will usually urge you to "update" or "validate" your account information and will often threaten some dire consequence for not responding to them. Be on the lookout for poor grammar or typographical errors. Many phishing emails are translated from other languages or are sent without being proofread, and as a result may contain bad grammar or typographical errors.

What do I do if I get a Phishing Email? --If you get an email that asks for sensitive information, do not reply or click on the link in the message. When possible, you should avoid clicking links in the email. Instead of clicking the link, type the URL into the address area of your Internet browser. At no time should you cut and paste the link included in the message. The phishing websites are cleverly constructed at times and will actually have a URL that begins with https like a secure server site does. The one tip off on not being a secure server site is there will not be the padlock indicator on the lower toolbar of your monitor.

The Federal Trade Commission has issued a warning about these identity theft scams. They suggest the following:

If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead,

contact the company cited in the email using a telephone number or Web site address you know to be genuine. Avoid emailing personal and financial information; always keep your password secure. Never share your password with anyone; always review your credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your credit card or bank statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.