Identifying Spoofed E-mails and Phishing Exploits

From time to time, you might receive e-mails that look like they come from a legitimate person (a prospective boat buyer, for instance), but instead are falsified. Such spam e-mails might ask about your boat in a vague and seemingly odd manner, with an indeterminate purpose, asking for you to respond. Or perhaps the e-mail directs you to a web site that looks something like a Catboat Association site, where you might be asked to provide account information such as your e-mail address and password combination.

Unfortunately, these false e-mails and web sites can be part of criminal exploits to steal your sensitive information; later, this information may be used to commit identity fraud or steal money from you. Some phishing messages contain potential viruses or malware that can detect passwords or sensitive data. We recommend that you install an anti-virus program and keep it updated at all times, along with some type of firewall (i.e., Windows Firewall/Security or Zonealarm). These are the first layer of defense for your computer's "perimeter".

Below are some key points to look for in order to identify these e-mails:

1. Requests to verify or confirm your account information

CBA will *not* ask you to verify or confirm your account information by clicking on a link from an e-mail.

2. Suspicious E-mails and Attachments

We recommend that you be wary of e-mails with odd messages, requests, or instructions. Do not open any e-mail attachments from suspicious sources. E-mail attachments can contain viruses that may infect your computer when the attachment is opened or accessed. If you receive a suspicious e-mail that contains an attachment, we recommend that you delete the e-mail and do *not* open the attachment.

3. Grammatical or typographical errors

Be on the lookout for poor grammar or typographical errors. Some phishing e-mails are translated from other languages or are sent by automated programs without being proofread, and as a result, contain bad grammar or typographical errors.

4. Check the Web site address

Genuine CBA web sites are always hosted on the "catboats.org" domain, such as "http://www.catboats.org/. . ." (or "https://old.catboats.org/cats4sale/. . ."). Sometimes the link included in spoofed e-mails looks like a genuine CBA address. You can check where it actually points to by hovering your mouse over the link – and the actual web site (where it points to) will be shown in the status bar at

the bottom of your browser window or as a pop-up.

We *never* use a hyphenated web address such as "http://security-catboats.org/. . ." or an IP address (string of numbers) followed by directory references (such as "http://123.456.789.123/catboats/. . . .").

Alternately, sometimes the spoofed e-mail is set up such that if you click anywhere on the text you are taken to a fraudulent web site. CBA will never send an e-mail that does this. If you accidentally click on such an e-mail and go to a spoofed web site, do not enter any information. For your protection, simply delete the email or close the browser window.

5. Do not "Unsubscribe"

Never follow any instructions contained in a forged e-mail that claim to provide a method for "unsubscribing." Many spammers use these "unsubscribe" processes to create a list of valid, working e-mail addresses.

6. Protect your account information

If you did click through from a spoofed or suspicious e-mail and you entered your personal information or submitted a credit card number, then you should immediately take steps to protect your information. You may wish to contact your credit card company, for example, to notify them of this matter.

(Close this window to close this document when finished reading.)