

## **Beware of Phishing, Vishing & Smishing**

You can avoid being “hooked” by phishing, vishing and smishing by staying on the lookout for fraudulent e-mails, voice messages and text messages.

*Phishing* is the practice of sending an e-mail that appears to be from a financial institution, an online store, or another organization with the goal of persuading online banking users to share sensitive information by clicking on a link or simply responding to the e-mail.

Vishing is like a traditional phishing scam. But instead of being directed to an Internet site, you’re asked to provide the information via a cell phone and given a number to call. This message could come from a live person or a pre-recorded message.

Smishing is also a lot like phishing & vishing but is sent via text message on your cell phone asking you to reply to the message.

Cyber-criminals use the personal information they gain to commit identity theft or fraud.

Over time, cyber-criminals have learned to create messages that can seem to genuinely come from the legitimate site. They may “borrow” a company logo, copy the format and colors used on its Web site, or imitate the language used in the organization’s real communications.

Remember that we will **never** ask you to click on an e-mail link to share sensitive financial information. If you receive an e-mail or other message that claims to be from Garden Island FCU or from any other financial institution and asks you to share account numbers, Social Security numbers, passwords or other personal information, **DO NOT RESPOND**. Please report it to us immediately. Other suspicious e-mails or Web sites should be reported to the companies involved.

If you responded to any messages by giving out personal information call us immediately at 245-2712. We will give you instructions for changing your password and taking other steps to protect your accounts.

### **Five Rules for Online Safety**

1. **Never** click on e-mail links.
2. Enter Web addresses in the browser bar instead of using e-mail links.
3. Never share financial or personal information by e-mail or text message.
4. Tell us about suspicious e-mails that contain our name or logo.
5. Check accounts regularly to spot fraud or unauthorized account access.

**In addition, please report Phishing Email. For instructions please go to their website [www.antiphishing.org](http://www.antiphishing.org).**