One booming business in the fading U.S. economy is email fraud. Online criminals are using concern about the economy and chaos in the financial markets as an opening to defraud worried consumers.

These new scams typically offer anxious consumers relief from tax bills or an alleged chance to protect their savings from loss or seizure.

The scammers send emails in which they pose as a financial institution, government agency, or credit counseling service. They entice consumers to provide sensitive information, such as social security numbers, account numbers and passwords. Although they promise consumers relief, these “phishing” scams are actually designed to use their personal information to steal from them.

“Be skeptical of any non-Certified email that asks for sensitive financial information or asks you to click on a link,” said Peter Horan, chief executive officer of Goodmail Systems. “These emails could either be taking you to a site that is trying to steal your information or will download spyware onto your computer that will surreptitiously transmit personal information to criminals.”

One current phishing tax scam features emails with the subject line “Who wouldn’t jump at a little extra money from the Internal Revenue Service?” The body of this email includes a realistic looking but fake IRS logo and falsely tells recipients that they are entitled to a refund. The phishing site to which recipients are directed, requests social security numbers, as well as bank information, both of which can lead to identity theft and financial fraud. Similar scams are being spread offering property tax relief.

Another type of email scam making the rounds this season tells taxpayers that they are entitled to a “stimulus payment” from the government. These emails “inform” recipients that their fiscal activity for the last year has been reviewed, and they are “eligible for a stimulus payment.” The email urges the recipient to fill out and return an attached form, which then asks for sensitive financial information. Obviously it’s all a scheme to steal information.

What can you do to protect yourself?

First, check to see if that email is valid. One way to tell is to look for the blue ribbon envelope seal next to an email message in your inbox. This indicates the email is a Goodmail CertifiedEmail, which means it is authentic and that you're safe to click on the links within it. Many government agencies and tax preparers use Certified Email to let you know their emails are safe.

If you think an email requesting action on a bank or investment account might be legitimate, it's always best to type the Web site address directly into the address bar of your browser. Consumers also can contact the government agency, bank or financial institution directly by phone or email with any questions.

Suspected tax fraud can be reported to the IRS using IRS Form 3949-A, which is available for download from the IRS Web site at IRS.gov, or through the U.S. Mail by calling 1-800-829-3676. The completed form or a letter detailing the alleged fraudulent activity should be addressed to the Internal Revenue Service, Fresno, CA 93888.