

HELP NET SECURITY

Get the facts about Extended Validation SSL Certificates from VeriSign

HOME NEWS ARTICLES SOFTWARE VIDEOS VULNS EVENTS NEWSLETTERS STORE



SUBSCRIBE BY E-MAIL

NEWS ARTICLES THE WIRE

- New book: "iPhone Forensics"
- Tumbleweed files patent infringement suit against Sendmail, Inc
- VMware patches critical openwsman security issues
- Apple updates security with Mac OS X 10.5.5
- Real time global view of your server network



GRAB OUR RSS FEED

DTrace

REVIEWS MALWARE

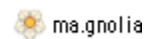
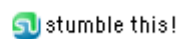
- Security Power Tools
- Network Warrior
- Google Apps Hacks
- Crimeware: Understanding New Attacks and Defenses
- Big Book of Windows Hacks

WINDOWS LINUX OS X

- LANguard Network Security Scanner 8 ***
- GFI MailEssentials 14
- Data Guardian 1.5.2

Consumer alert: Beware of email scams tied to financial crisis

Posted on 19 September 2008.



Goodmail Systems, creators of CertifiedEmail are advising consumers to be on the lookout for fraudulent email scams and "phishing" attacks related to the current turmoil in the U.S. financial and insurance markets. Email scammers like to use global crises and high profile news headlines when baiting consumers. In the wake of Hurricane Katrina, millions of Americans received fake emails claiming to be from charitable organizations soliciting donations. When the government distributed stimulus checks earlier this year, the IRS became the target. Phishers know how to make use of people's vulnerabilities during times of stress.

Phishing is one form of email fraud in which the scammer impersonates a bank, non-profit or other company a consumer does business with, like a travel company, retailer or news media outlet. By pretending to be a company the consumer trusts, or by offering a special deal to a consumer, the scammer is able to obtain sensitive personal information which can lead directly to embezzlement.

Banks, retailers, news companies and others who have been "spoofed" by scammers are beginning to use more advanced systems of assuring consumer confidence. CertifiedEmail is a separate class of "digitally signed" messages that assures a message is really from the sender it seems to be from. CertifiedEmail messages are marked with a blue ribbon envelope in the mail interface letting a consumer know the message is safe and authentic.

Unless consumers are certain of the sender's identity, consumers should consider the following tips in the event that they receive emails related to the current financial crisis:

1. If You're Not Sure It's Real, Pick Up the Phone.

Phishers are experts at visually mimicking brands' identities and can even forge the "From" line to make their emails seem like they're coming from a legitimate source. Unless you see the blue ribbon envelope of a CertifiedEmail, you may not be able to tell

- Kerio WinRoute Firewall 6.5.0 Build 4794
- AutoKrypt 8.06
- BestCrypt 8.05.5

- ADVISORIES** **VULNERABILITIES**
- Debian Security Advisory - wordnet (DSA-1634-)
 - Debian Security Advisory - horde3 (DSA-1642-)
 - Debian Security Advisory - phpmyadmin (DSA-1641-1)

whether an email is real. If you are suspicious, call customer service - they will help you determine whether what you received was legitimate or a fraudulent phishing scam.

2. Be Skeptical of Requests for Personal Information.

Never reply to emails asking you to update personal identification

3. Don't Click Links.

Clicking on links in fraudulent emails often take recipients to corresponding phishing Web sites where sensitive personal data is collected. Even worse, visiting these illegitimate sites can sometimes launch the installation of viruses, keystroke loggers and other malicious code onto users' computers. Unless a message is a CertifiedEmail, you should manually type the URL of the company you do business with into your Web browser, rather than clicking on a link in the message.

4. Delete All Attachments.

Opening attachments is an even bigger no-no than clicking on links. They can be highly insecure and no company you do business with will ever send them to you.

5. Report It.

Help law enforcement and organizations stop phishing attacks from affecting other potential victims. Send the phishing email, including the full header, to the Anti-Phishing Working Group (APWG) at reportphishing@antiphishing.org. APWG is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.

Qualys: This free security guide describes the scanning requirements for PCI-DSS and provides a quick-reference requirements matrix for both Merchants and Service Providers of all levels.



GFiMailEssentials
for Exchange/SMTP/Lotus

[Download a free trial](#)

COPYRIGHT 1998-2008 BY HNS CONSULTING LTD. // READ OUR PRIVACY P