Alert2Fraud

FRAUD RESOURCE GROUP

FRAUD AWARENESS INFORMATION AT YOUR FINGERTIPS

3rd Quarter '06

**Welcome to Alert2Fraud!**

Some readers prefer to enlarge this page to 150% or more.

Each month, we shine a light on frauds and fraud trends that Internet users and businesses need to know.

Each Alert2Fraud edition is designed to be a quick but informative read.

Your comments and suggestions are welcome.

Please contact us at:
A2F@fraudresourcegroup.com

**Learn More…**

www.apwg.org

www.stopkeylogging.com

www.ftc.gov



# Vishing – Dialing for Dollars

**Fraud:** The advent of Voice over Internet Protocol (VoIP) has fueled an industry boom. Unfortunately, the booming industry to which I'm referring is FRAUD!

VoIP allows telephone calls to be made over high speed Internet connections and has quickly gained popularity because it is relatively inexpensive and piggy-backs on a technology that many people are already paying for - their broadband Internet service.

By its nature, VoIP also provides anonymity to its users. Add all of these elements together and you can begin to understand why VoIP has become a powerful new means of manipulating victims into divulging sensitive account-related information.

Operating under the guise of protecting the users' online security, Vishing e-mail messages encourage individuals to call a toll-free number to update their account information instead of clicking on a link in an e-mail. This social engineering technique leads the user to believe that the solicitor is acting in his or her best interest and can lead to a false sense of security with passing sensitive information to the party on the other end of the call.

**Prevention:** As with suspected Phishing messages, if you receive a message to which you feel you need to respond, contact the entity by using a published phone number. Be suspicious of unsolicited messages that ask you to divulge sensitive information.

# Phishing - the Mother of Many Frauds

**Fraud:** Phishing, or the use of e-mail messages designed to lure unsuspecting computer users into divulging sensitive password, user name and account information, is arguably one of the most successful fraud schemes in history.

Since surfacing just a few years ago, phishing has evolved from poorly-written e-mails with typographical errors and poor graphics to a growing family of often sophisticated schemes that has become increasingly more difficult to discern as fraudulent.

In the course of a year, hundreds of billions of dollars will have been lost to these fraud schemes and many of the individuals left in their wake have become identity theft victims.

As well, many more recent Phishing messages contain Trojan horses that secretly deposit keystroke loggers onto unsuspecting users' computers.

These malicious code-laced messages effectively steal the data that they can't otherwise entice their users to divulge, using their own Internet or Instant Message (IM) programs to send the stolen data to the keyloggers' handlers.

**Prevention:**

- Enable your Spam Filter and update your anti-virus software.
- Never click on a link within an e-mail received from an unknown sender.
- If you receive a message to which you feel you need to respond, find a published phone number or contact e-mail address to use.
- Delete suspect messages completely from your computer.