

Consumer ALERT



ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

“Vishing” is a New Addition to Identity Thieves’ Arsenal

In a new twist to an ongoing scam, consumers’ identities and personal information could be stolen by “vishing.”

“Phishing” scams have been around since the early days of the Internet. They involve sending an email that looks as if it’s from a legitimate bank or merchant asking consumers to re-submit their personal information. Generally, phishing scam emails are intended to cause alarm by telling the consumer that they must re-submit personal information immediately or their accounts will be “suspended.” Consumers are then typically asked to click on a link that takes them to a legitimate-looking Web page in which they are asked to re-submit their personal information, such as account number and passwords.

In a new twist, “vishing” takes advantage of even newer technology to defraud unsuspecting consumers. Like with phishing scams, vishing typically starts with the same alarming email which appears to be from a legitimate business or banking institution. But rather than instructing consumers to re-submit their personal information online, vishing emails tell the victim to call a phone number through which they can provide their information. When the consumer calls, an automated message identifies itself as the bank or retailer that sent the original email and prompts the consumers to key-in their personal information. Once this information is entered, the scam artist will be able to access the consumer’s account or open lines of credit in his or her name, thus causing considerable harm.

Consumers who by now are wary of dubious emails that link to bogus Web pages might not be as reluctant to call a phone number, especially if it appears to be a local call. However, identity thieves who perpetrate vishing often use new technology that enables them to subscribe to Internet-based phone service via **Voiceover Internet Protocol (VoIP)**. This makes it possible for a scam artist thousands of miles away to set up a phone account that victims might believe is a local call. But just as in a phishing scam, victims will be submitting their sensitive information to a thief beyond the reach of law enforcement in the United States.

**WRITE TO: Greg Abbott, Office of the Attorney General, PO Box 12548,
Austin, TX 78711-2548 • (800) 252-8011 • www.oag.state.tx.us**

The warning remains the same: *Never respond to an email that purports to be from your bank or other business that threatens “suspension” of your account or a similar drastic action unless you immediately re-submit your personal information, either by clicking on a link or calling a phone number.* Legitimate businesses do not contact and threaten their clients in this manner. If you have any questions about such emails, contact the bank or business purportedly sending the email directly based on a phone number that appears in the phone directory or your statements. **DO NOT** call a phone number that appears on an email.

If you believe you have been the victim of identity theft, immediately file a report with your local law enforcement agency. You should also obtain an **ID Theft Victim’s Kit** through my office at **1-800-252-8011** or online at www.oag.state.tx.us for additional steps you should take to prevent further losses and clear your name.

Sincerely,

A handwritten signature in black ink that reads "Greg Abbott". The signature is written in a cursive, flowing style.

Greg Abbott
Attorney General of Texas

**WRITE TO: Greg Abbott, Office of the Attorney General, PO Box 12548,
Austin, TX 78711-2548 • (800) 252-8011 • www.oag.state.tx.us**