

Security Alert for Amegy Bank Customers

Our banking customers should be aware that fraudulent emails ("Phishing") are being sent to customers within some of the U.S. banks. The fraudulent emails are sent to random email addresses hoping to trick customers into revealing their account and electronic banking logon details.

Although Amegy Bank has no reports of its customers being affected, we want you to be aware of this scam, which can be easily avoided.

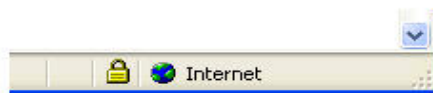
How does it work?

A fraudulent email would look like an email from Amegy Bank asking you to follow a link in the email to log on to e-banking and reactivate your logon or account details. It may ask you to provide your Access ID, your PIN or other financial details.

If you click on the link within the fraudulent email, you will be taken to an imitation website that looks similar to the Amegy Bank website. Any details you provide to that site may then be collected and used without your knowledge.

How to protect yourself

- Never follow links to Amegy Bank e-banking from an email you have received.
- Always log on to Amegy Bank's e-banking by typing www.amegybank.com into your address bar, or by bookmarking our site in your "Favorites".
- Amegy Bank's authentic "Logon" page will always feature a small yellow padlock at the bottom right corner of your web browser. The padlock symbol indicates that the page you are on has additional security (digital security). You can double-click on it to confirm that the certificate of authenticity has been issued by "www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign" to "www.amegybank.com".



- Amegy Bank's Bill Pay certificate of authenticity has been issued by "www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign" to "billpay.amegybank.com"
- The newest Phishing scams use a special program (Java) to present a URL that you may think is legitimate. The only way to make sure it is legitimate is to verify the certificate. **Always** check the yellow padlock to display the certificate's credentials and compare them to what you would expect to see. Phishers are now obtaining digital certificates from unofficial Certificate Authorities, they just use self-signed or bogus or even stolen certificates. If the web browser displays a warning that the certificate does not match the server registered – DO NOT IGNORE the warning and do not access the site.
- Ensure your computer is protected by up-to-date anti-virus and personal firewall software.

- Only conduct financial transactions online using computers you know are secure. This means that use of internet cafes should be avoided.
- Never leave your computer unattended while logged on to electronic banking.
- We strongly suggest that you do not share your Personal ID, Password, PIN or Account Number with anyone under any circumstances.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact Amegy Bank at 713.235.8810 and press option 10 and speak to a customer service representative.
- Ensure that your browser is up to date and security patches applied. In particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page -- <http://www.microsoft.com/security/> -- to download a special patch relating to certain phishing schemes.
- Do not provide your e-mail address to third party web sites without reading their privacy and security policies and terms and conditions to ensure you understand the circumstances in which your e-mail address can be used.

You should immediately be suspicious of any phone call, email or correspondence which asks you to disclose your banking details. Amegy Bank or its staff should **never** ask you for your PIN (although in some circumstances we might ask you to verify your Access ID).

If you have replied to a suspicious e-mail and provided personal or sensitive information about your account, please contact us immediately at 713.235.8810 and press option 10 and speak to a customer service representative.

You can report "phishing" or "spoofed" e-mails to the following groups:

- Forward the email to reportphishing@antiphishing.com
- Forward the email to the Federal Trade Commission at uce@ftc.gov
- Forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
- When forwarding spoofed messages, always include the entire original email with its original header information intact
- Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/