

What is Phishing?

Phishing is the use of fraudulent e-mail that appears to come from your bank or another trusted business, but actually is from an imposter. Such e-mail asks customers to verify personal information or links to counterfeit websites that appear real.

How to Recognize Phishing

Watch for e-mail that:

- Urges you to act quickly because your account may be suspended or closed.
- Doesn't address you by name, but uses a more generic title like "Dear valued customer."
- Asks for account numbers, passwords or other personal information.

Remember, businesses such as your bank or credit card provider will never ask you for personal information, such as account numbers or passwords, in an e-mail. Do not respond to any e-mail that directs you to update your personal information online or by dialing a telephone number. Use only the customer service numbers listed on your statements.

How to Prevent Phishing

- Ensure that your virus scanning software automatically scans attachments, or scan them manually prior to opening them.
- Verify that the e-mail sender's address is what you would expect.
- Be suspicious of e-mail attachments from a stranger. If you don't know or recognize the sender, do not open the attachment.
- Do not reply to e-mail requests for financial information if you suspect the message might not be legitimate.
- Never send confidential information, such as account numbers or passwords, in an e-mail.
- Always use an up-to-date browser with at least 128-bit encryption.

Helpful Resources

Links to third-party sites are provided for your convenience.


- Anti-Phishing Working Group (<http://antiphishing.org>): Association focused on eliminating fraud and identity theft.
- Better Business Bureau Phishing Facts (<http://www.bbbonline.org/idtheft/phishing.asp>): Shows latest news and alerts.
- FDIC (<http://www.fdic.gov/consumers/consumer/alerts/phishing.html>): Phishing Consumer alerts.



Watch for e-mails that don't address you by name, but use a more generic one like "Dear valued customer."

Watch for e-mails that ask for account numbers, passwords or other personal information.

-----Original Message-----
From: USAA Bank [mailto:noreply@usaa.com]
Sent: Monday, November 14, 2005 4:52AM
Subject: USAA Bank : Internet Banking



Dear USAA Bank Customer:

For your security, the profile that you are using to access USAA Online Banking has been locked because of too many failed login attempts.

You can unlock this profile online by selecting an option below:


Unlock your profile with:
[My ATM/Visa Check Card number and PIN.](#)
[Other personal information \(Social Security Number, Account #, etc\) E-mail address](#)

We regret any inconvenience this may cause you.

Sincerely,
USAA Bank Account Review Department.

We are requesting this information to verify and protect your identity. This is in order to prevent the usaa of the U.S, banking in terrorist and other illegal activity.

Please do not "Reply" to this Alert.



9800 Fredericksburg Rd.
San Antonio, Texas, 78288-001

Copyright © 1997-2005, USAA. All Rights Reserved.