

PHISHING SCAM—SAMPLE 1

I don't even bank with SCAMBank! Why are they emailing me? THEY'RE NOT! IT'S A SCAM!

A real bank won't email asking for your personal information. This email is from scammers pretending to be a legitimate bank. They are 'phishing' for your personal information, like your bank account details, passwords and credit card information which they will use to steal your money!

NEVER GIVE OUT YOUR PERSONAL INFORMATION BY EMAIL! IF YOU RECEIVE AN EMAIL LIKE THIS DELETE IT! Check out **SCAMwatch** for help

Looks official—it must be genuine —NOT TRUE!

Phishing scams use official-looking logos, letterheads and language to trick you into believing its real. These things are easily copied and forged.

From: SCAMBank Customer Service [mailto:no_reply@accuvant.com]
Sent: Wednesday, 30 January 2008 6:32 AM
To: john citizen
Subject: Spam: SCAMBank. Official notice - ONW3329389

SCAMBank

DON'T PANIC! The bank hasn't really suspended your account!

Scammers scare you into believing that your bank has closed your account and that you can't access your money. **THIS IS NOT TRUE!** Scammers will try to trick you into giving them your personal information.

Dear Customer,

SCAMBank temporarily suspended your account. Reason: **Billing failure**. All restricted accounts have their **billing information unconfirmed**, meaning that you may no longer send money or withdraw cash from your account until you have updated your billing information on records.

Wouldn't my bank have my details backed up?

Real banks and financial institutions have protection so they don't lose your details. Scammers are trying to get at your bank account numbers, passwords and credit card details so that they can steal your money or your identity!

DON'T RESPOND!

To initiate the update confirmation process please **follow the link below and fill in the necessary requirements:**

[Click here.](#)

NO! DON'T CLICK! This link will take you to a fake webpage—it may look like the real thing but it isn't!

Links might also download spyware to your computer so that scammers can collect all your passwords and other personal details.

DON'T FOLLOW ANY LINKS OR GIVE OUT ANY INFORMATION!

This link will take you to a fake webpage set up by scammers to trick you into giving them your information—it may look like the real thing but it isn't.

NO IT WON'T! Scammers will use your personal details to steal money from your bank accounts or steal your identity. Scammers will also give your details to other scammers who will also target you. DELETE IT!

We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation.

Remember, we are committed to your security and protection. To find out more, **take a look at our Security section on the Web site.**

The **information provided will be treated in confidence and stored in our secure database.**

If you fail to provide information about your account you'll discover that your account has been automatically deleted from SCAMBank database.

Please call us on **1111 123 456 789** if you have any queries

'Quick! before it's too late!' DON'T RESPOND! THIS IS A TRICK!

Scammers will use threats to scare you into providing your personal details. Remember, a legitimate bank or financial institution will never threaten to close your account by email.

NEVER CALL A NUMBER LISTED IN THE EMAIL!

If you think the email could be genuine, find the bank's real telephone number from the phone book or from a bank statement or card, and ask them for their advice. Many banks have specialised internet security staff who can help you.

Copyright © 2008 **SCAMBank Banking Corporation PTY LTD**

--

The contents of this email and any attachments are sent for the personal attention of the addressee(s) only and may be confidential. If you are not the intended addressee, any use, disclosure or copying of this email and any attachments is unauthorised - please notify the sender by return and delete the message. Any representations or commitments expressed in this email are subject to contract.

Looks official—it must be genuine! NOT TRUE!

Scammers use official language and company information to trick you. Don't be fooled, these things are easily copied!