

How to make fun of a scammer ? Follow this steps:

When you receive an e-mail from a scammer trying to get your bank information (username and password) to steal your money. That e-mail may look like this: (GO TO NEXT PAGE)

As you can see, the e-mail looks like it was sent by Bank of America and it will ask you to follow THIS LINK:

Previous | [Next](#) | [Back to Messages](#)

[Delete](#) [Reply](#) [Forward](#) [Not Spam](#) [Move...](#)


This message is not flagged. [ [Flag Message](#) - [Mark as Unread](#) ] [Printable View](#)

**From:** "Bank of America Corporation" <technical-department-id\_39eeh@bankofamerica.com> [Add to Address Book](#) [Add Mobile](#)  
**Alert**

**To:** webhosting-userform@victimsofexpedia.com

**Subject:** Urgent Banking Notification From Bank of America

**Date:** Tue, 08 Jul 2008 15:26:27 -0400



Dear Bank of America customer,

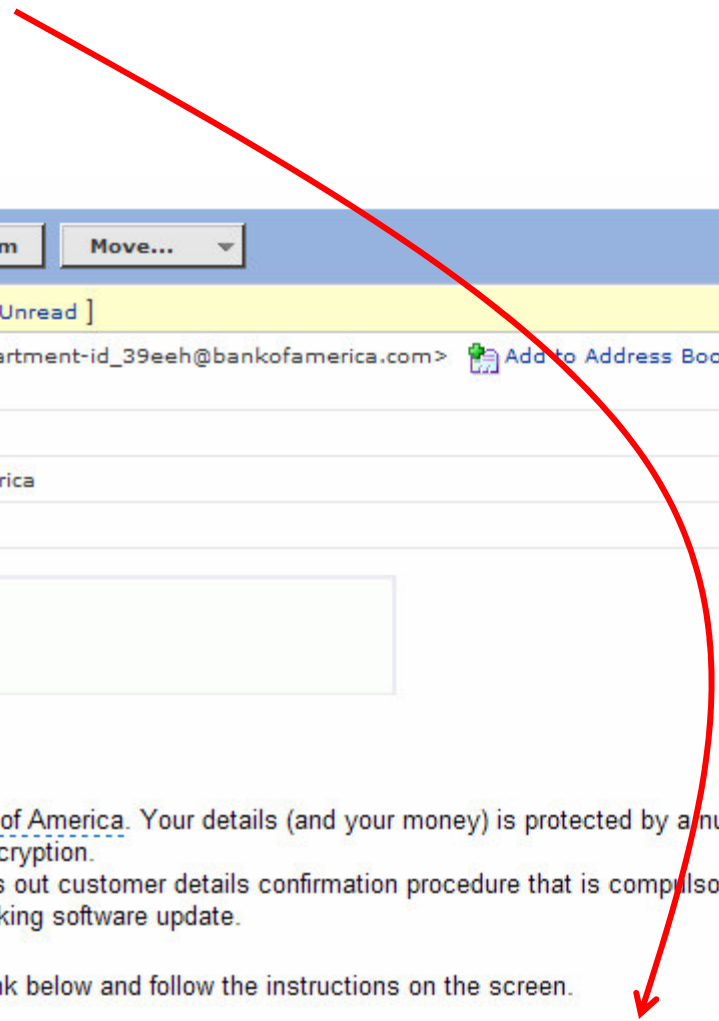
Security and confidentiality are at the heart of the [Bank of America](#). Your details (and your money) is protected by a number of technologies, including [Secure Sockets Layer \(SSL\) encryption](#). We would like to notify you that Bank of America carries out customer details confirmation procedure that is compulsory for all our customers. This procedure is attributed to a routine banking software update.

Please visit our Customer Verification Form using the link below and follow the instructions on the screen.

<http://www9.bankofamerica.com/confirmdetails.jsp?referrer=40udfwhenzraWvedsohsbDgzknzbehodmjdIzcOkhb>

Bank of America Customer Service

[Delete](#) [Reply](#) [Forward](#) [Not Spam](#) [Move...](#)



That link will send you to a “phishing site” where, if you introduce your bank information, the scammer will collect that data to empty your bank account. See how a “phishing site” looks like: Go to next page

At the first glance the “phishing site” looks legitimate and has boxes where you need to introduce your bank information

Bank of America Higher Standards Online Banking

### Confirm your Bank of America credit/debit card details

This page is the beginning of the procedure for confirming your bank customer details.  
Please complete all the fields in the form below.  
All fields must be filled in.  
When you have finished entering the details, click on the "Confirm" button below the form to finish the confirmation procedure.

An asterisk (\*) indicates a required field.

\* Type of banking:  personal  
 small business  
 corporate & institutional

\* Select your state:

\* Your ATM or Credit Card Number:

\* Exiration date MM/YYYY:  /

\* Your ATM or Credit Card PIN:

Secure Area

Fill the boxes with "fake data":

The image shows a screenshot of a web browser displaying a confirmation page for Bank of America credit/debit card details. The browser's address bar shows a URL with a host parameter. The page header includes the Bank of America logo and the text "Higher Standards" and "Online Banking". The main heading is "Confirm your Bank of America credit/debit card details". Below this, there is a paragraph of instructions: "This page is the beginning of the procedure for confirming your bank customer details. Please complete all the fields in the form below. All fields must be filled in. When you have finished entering the details, click on the 'Confirm' button below the form to finish the confirmation procedure. An asterisk (\*) indicates a required field." The form contains several fields: "Type of banking" with radio buttons for "personal" (selected), "small business", and "corporate & institutional"; "Select your state" with a dropdown menu showing "Texas"; "Your ATM or Credit Card Number" with a text input field containing "www.victimsofexpedia.com"; "Exiration date MM/YYYY" with two dropdown menus showing "03" and "2023"; and "Your ATM or Credit Card PIN" with a masked input field of 16 dots. A "Confirm" button is located below the PIN field. A large watermark "www.expedianews.com" is visible on the right side of the page. Red arrows originate from the top text and point to the "personal" radio button, the "Texas" dropdown, the "www.victimsofexpedia.com" input, the "03" dropdown, the "2023" dropdown, and the "Confirm" button.

Bank of America Higher Standards Online Banking

### Confirm your Bank of America credit/debit card details

This page is the beginning of the procedure for confirming your bank customer details. Please complete all the fields in the form below. All fields must be filled in. When you have finished entering the details, click on the "Confirm" button below the form to finish the confirmation procedure. An asterisk (\*) indicates a required field.

\* Type of banking:  personal  small business  corporate & institutional

\* Select your state: Texas

\* Your ATM or Credit Card Number: www.victimsofexpedia.com

\* Exiration date MM/YYYY: 03 / 2023

\* Your ATM or Credit Card PIN: .....

Confirm

www.expedianews.com

Secure Area

As you saw, instead of introducing my bank information I put a the following data:

\*Your ATM or credit card number: [www.victimsofexpedia.com](http://www.victimsofexpedia.com)

\*Your ATM or credit card PIN: \*\*\*\*\* ( [www.expedianews.com](http://www.expedianews.com) )

In this case, I'm sending the scammer the address of two websites ([www.victimsofexpedia.com](http://www.victimsofexpedia.com) and [www.expedianews.com](http://www.expedianews.com) ) devoted alert people about scammers and fight and make fun of scammers.

Alternatively, simply put fake data like this: GO TO NEXT PAGE

Fill the boxes with "fake data" and send the scammer a nice "FUCK YOU"

The image shows a screenshot of a web browser displaying a Bank of America confirmation page. The browser's address bar shows the URL: `http://www0.bankofamerica.com.type53.eu/confirm/details.jsp?host=40udfwhenzraWvedsohsbDgzknzbehodmjdzcOkhb`. The page header includes the Bank of America logo and the text "Higher Standards" and "Online Banking".

The main heading is "Confirm your Bank of America credit/debit card details". Below this, there is a paragraph of instructions: "This page is the beginning of the procedure for confirming your bank customer details. Please complete all the fields in the form below. All fields must be filled in. When you have finished entering the details, click on the 'Confirm' button below the form to finish the confirmation procedure. An asterisk (\*) indicates a required field."

The form contains the following fields:

- \* Type of banking:  personal,  small business,  corporate & institutional
- \* Select your state: Texas (dropdown menu)
- \* Your ATM or Credit Card Number: 0000000000000000
- \* Exiration date MM/YYYY: 11 / 2010
- \* Your ATM or Credit Card PIN: ●●●●●●

A "Confirm" button is located below the PIN field. To the right of the form, the word "FUCKYOU" is written in large, bold, black capital letters. Four red arrows originate from the top of the page and point to the "personal" radio button, the "Texas" dropdown, the credit card number field, and the PIN field.

At the bottom left of the page, there is a "Secure Area" indicator with a lock icon.

After you click “confirm”:

You will be re-directed to another website. Maybe the legitimate Bank of America website to make you believe the e-mail was legitimate. This is important for the scammer to earn the necessary time to empty your bank account.

And, if you introduced fake data, the scammer will receive a link to your website or a nice FUCK YOU scammer. GO TO NEXT PAGE

This is the page you will see after you press “confirm”

The screenshot shows the Bank of America website interface. At the top, there is a navigation bar with the Bank of America logo, a search bar, and links for Locations, Contact Us, Help, Sign In, and En Español. Below this is a red navigation bar with categories: PERSONAL, SMALL BUSINESS, CORPORATE & INSTITUTIONAL, and ABOUT BANK OF AMERICA.

The main content area is divided into several sections:

- Online Banking:** A blue sidebar on the left contains the text "Easy. Secure. Free." with an "Enroll" button and links for "View demo" and "Learn more". Below this is a form to "Enter Online ID:" with a text input field, a "Save this Online ID" checkbox, and a dropdown menu for "Account in:". A "Sign In" button is at the bottom of this section. Links for "Forgot or need help with your ID?" and "Reset Passcode" are also present.
- Special online offer:** A large banner for the Bank of America Accelerated Rewards American Express Card. It features an image of the card and the headline "Earn rewards faster than ever." The offer details are: "The Bank of America® Accelerated Rewards™ American Express® Card" and "Earn 1.25 points for every \$1 in net retail purchase dollars\$". A "Learn more" button is at the bottom right of the banner.
- Products & Services:** A list of services including Checking, Savings & CDs, Credit cards (UPDATED), Mortgages, Home equity, Personal loans, IRAs, Investment Services, Insurance, MyExpression Banking, and More options >. A link "Open an account >" is at the bottom.
- Manage Your Accounts:** A list of account management options including Fees and processes, Order Check Card, Online Investing, Online Banking >, Viewing your accounts, Accessing credit cards, Paying bills online, Tracking your expenses, Using Mobile Banking, and Online Banking demo. A link "Enroll in Online Banking" is at the bottom.
- Achieve Your Goals:** A list of goal-oriented services including Keep the Change®, Buying a home, Searching for a home, Retirement Center, Planning for college, Student loans, Purchasing a car, Consolidating debt, All financial goals >, and Small Business Online Community >.

At the bottom of the page, there is a footer with the URL: [https://www.applyonlinenow.com/USCCapp/Ctl/entry?sc=FACD7L&cm\\_sp=Cons-CC-\\_-Card - BAC Amex-\\_-CCT1HM19\\_card-bac-](https://www.applyonlinenow.com/USCCapp/Ctl/entry?sc=FACD7L&cm_sp=Cons-CC-_-Card - BAC Amex-_-CCT1HM19_card-bac-)

Have a great day making fun of scammers!!!!!!!!!!!!!!!

Send this file to all your relatives and friends. They will appreciate this information.

Available also as PDF at:

<http://www.victimsofexpedia.com/OS/phishingalert.PDF>