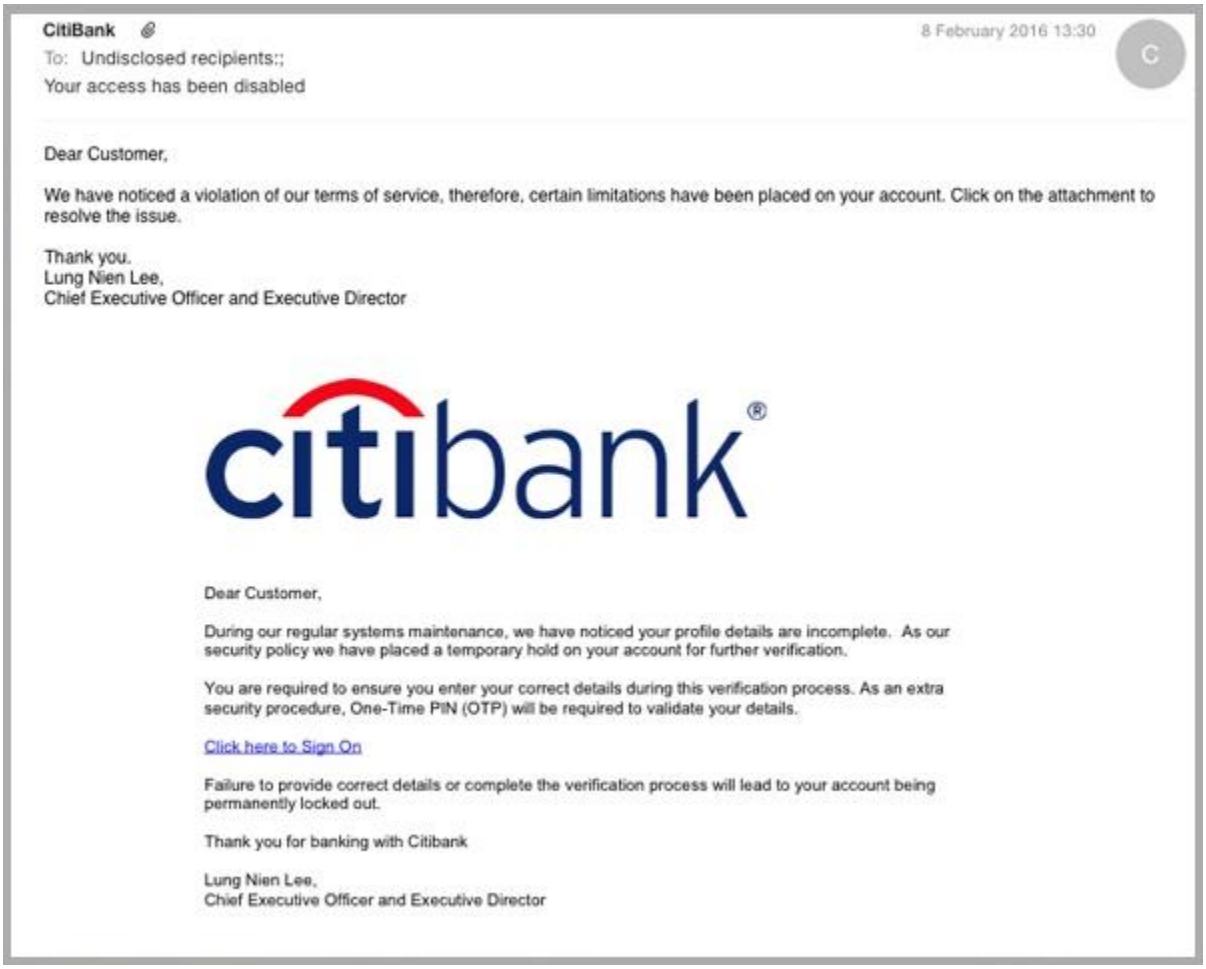
A new fake Citibank phishing scam using advanced techniques to manipulate users into surrendering online banking access has emerged.

The Citibank scam tricks users into surrendering their online banking username, password, and additional one-time pin (OTP) verification code.

Here's a sample of the email you should look out for:



CitiBank

8 February 2016 13:30

To: Undisclosed recipients:;

Your access has been disabled

Dear Customer,

We have noticed a violation of our terms of service, therefore, certain limitations have been placed on your account. Click on the attachment to resolve the issue.

Thank you.
Lung Nien Lee,
Chief Executive Officer and Executive Director

citibank®

Dear Customer,

During our regular systems maintenance, we have noticed your profile details are incomplete. As our security policy we have placed a temporary hold on your account for further verification.

You are required to ensure you enter your correct details during this verification process. As an extra security procedure, One-Time PIN (OTP) will be required to validate your details.

Click here to Sign On

Failure to provide correct details or complete the verification process will lead to your account being permanently locked out.

Thank you for banking with Citibank

Lung Nien Lee,
Chief Executive Officer and Executive Director

As you can see, the Citibank email scam appears to originate from the American bank, with the scammers successfully forging the email header address to make it appear to originate from Citibank.

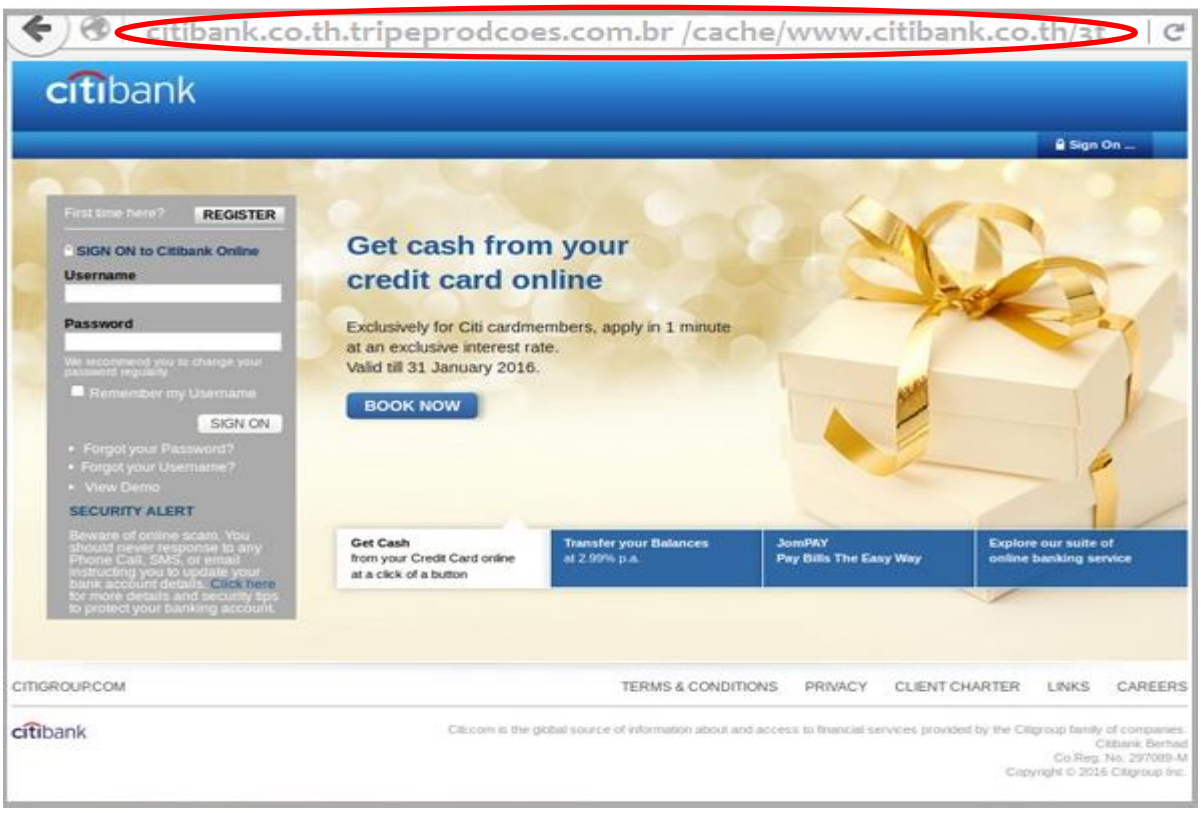
The email falsely advises recipients that their account access has been placed on hold until further verification has been provided.

In a change from many phishing emails which contain grammatical mistakes, the Citibank scam is written in impeccable English, although readers might be wary of an email which purports to be sent from the Chief Executive Officer, who wouldn't normally write to individual customer regarding everyday account issues.

The Citibank phishing email includes a PDF attachment, which asks users to click on an enclosed link to sign into their account.

Here scammers have tried to bypass traditional anti-virus filters which don't scan for malicious links held within email attachments.

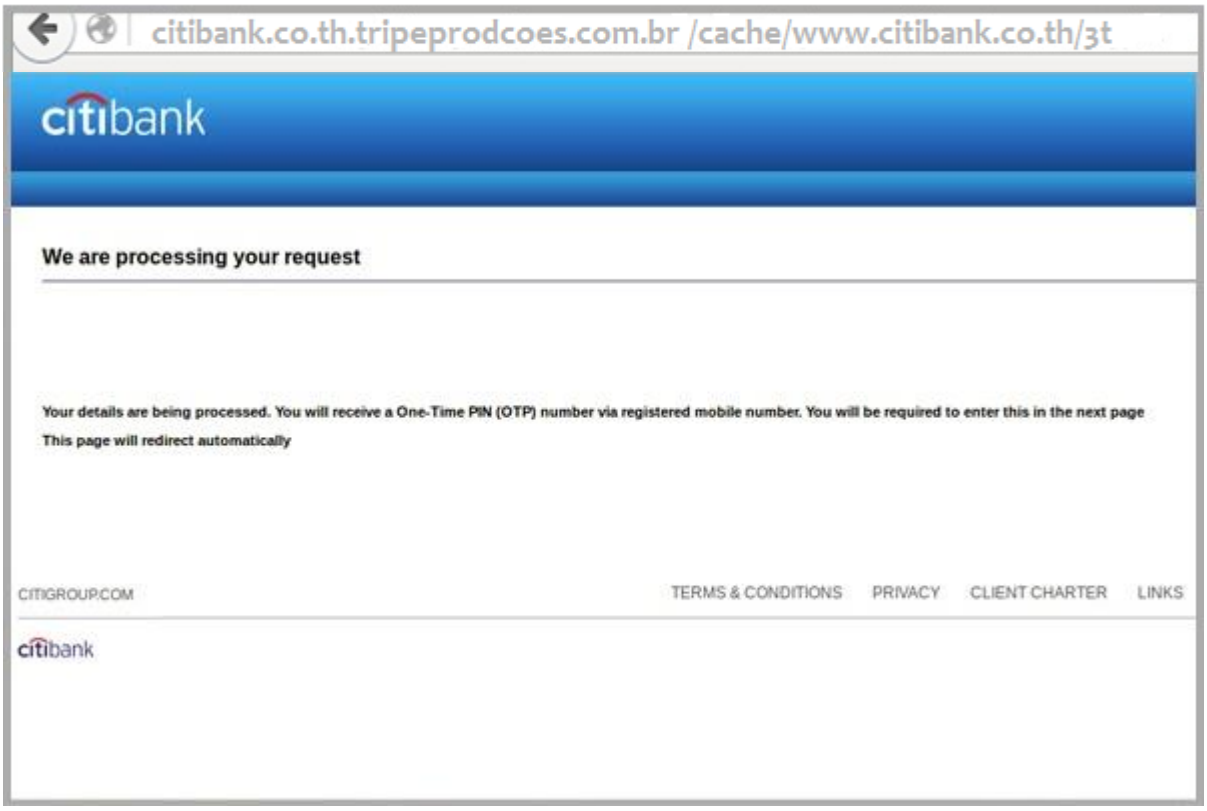
Once the user has clicked on the link in the PDF document, they are then directed to a fake Citibank landing page, which is a direct replica of the American Bank's internet banking log-in page:



As you can see from the URL in the address bar, the scammers have tried to fool the reader into thinking it's a legitimate Citibank webpage by appending a subdomain relating to the American bank.

However, your internet browser should normally highlight the true website address or domain, in this case ***tripeprodcoes.com.br,*** a website hosted in Brazil.

The user is encouraged to enter their username and password to gain access to their internet banking account, before being directed to the below page:



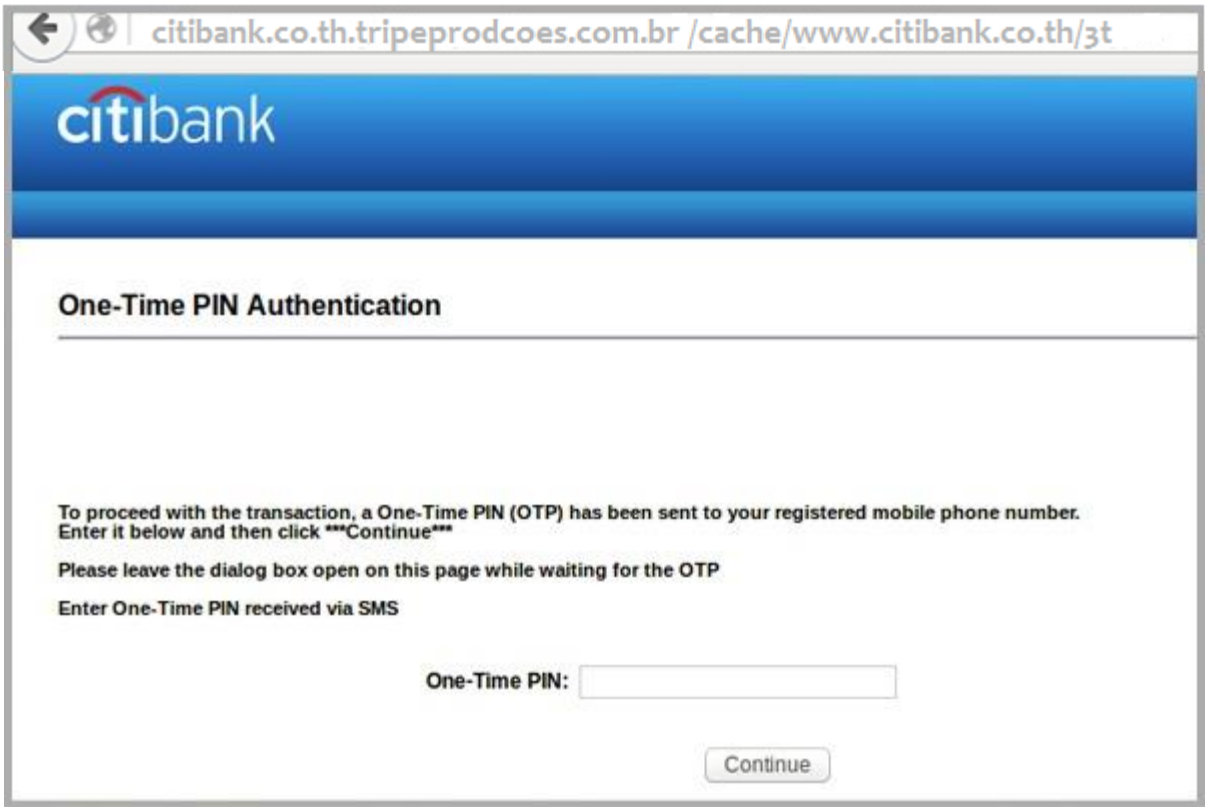
Now this is where the scam gets interesting: the scammers advise that a One-Time PIN (OTP) number has been sent to the banking user's mobile phone, as a way of verifying your account details.

OTP is the second stage of a two-part authentication process which Citibank uses to allow customers to perform a range of online transactions securely.

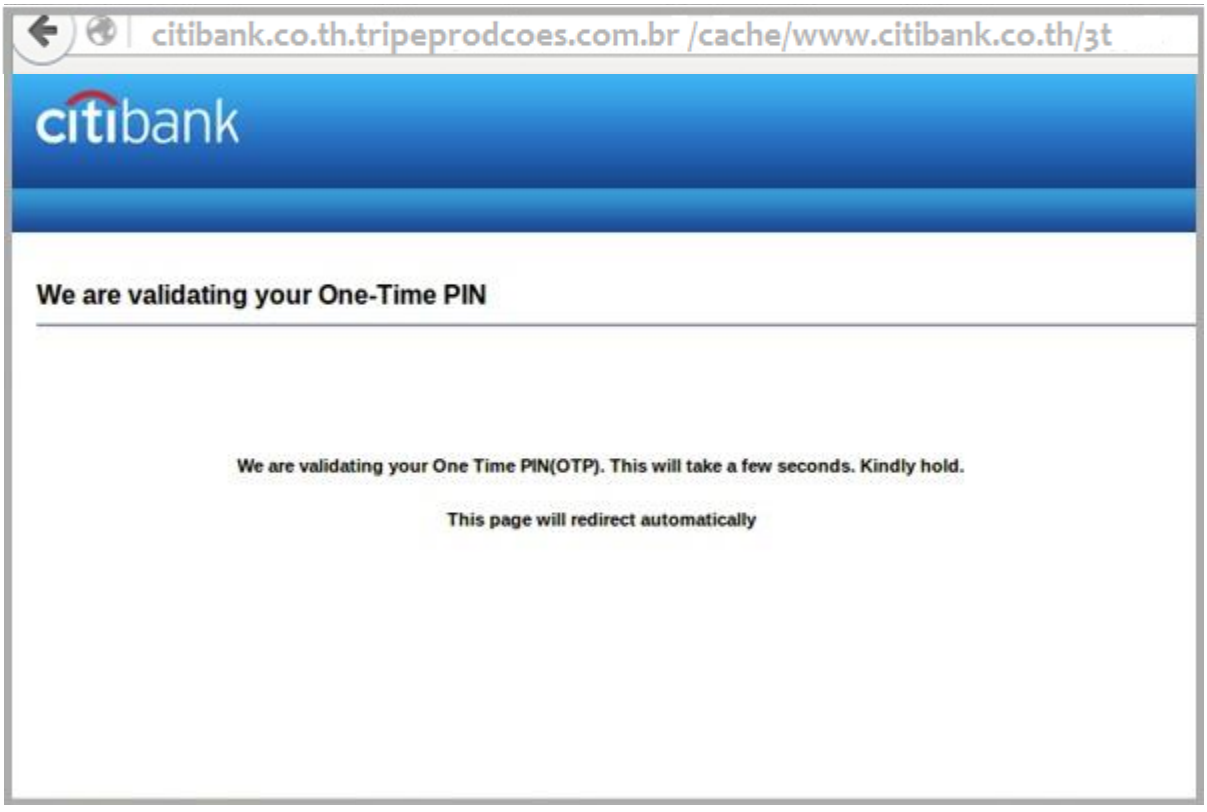
By setting up automated code in the background, the scammers are able to log into the user's official Citibank internet banking page on their end in real-time, using the account username and password details submitted in the previous screen.

It's likely that they will then attempt to perform a transaction on the user's account, which will result in Citibank sending an OTP code to their phone.

The above page then remains active for a set amount of time, giving enough time for the authentication code to be sent to the user's phone, before redirecting to the below page, where they are asked to enter the OTP:



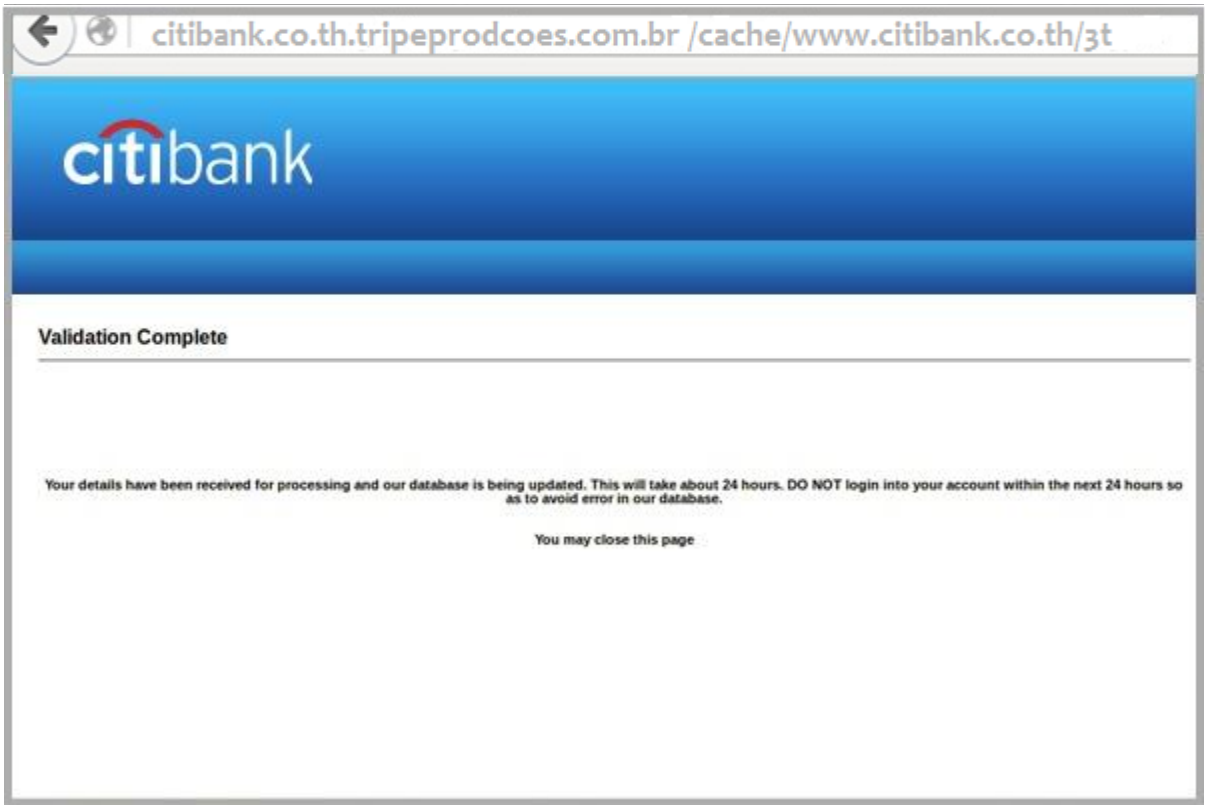
The reader is then told to hold while it authenticates, shown below, giving the scammers further time to access to the account, while the user is sitting at their computer screen waiting:



The subsequent pages in this Citibank scam ask the user to enter further OTP authorization codes, most likely in an attempt to get them to surrender additional verification information used for a range of different transactions.

For example, in order to transfer funds to a new payee, which the cyber-criminal would require to directly appropriate funds from your account, Citibank requires an additional 'OAC' code, also sent to the user's mobile phone.

The final page in the Citibank email scam warns that users shouldn't login to their online account for the next 24 hours in order to "avoid an error in our database":



This tactic could be used to delay the reader from logging into their accounts and finding out that funds have been transferred fraudulently to the cyber criminal's named account.

After all, the more time the scammer has to withdraw the funds, the less likely their bank is able to immediately revoke the transfer once the alarm's been raised.