



Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Citibank phishing baits customers with fake suspension alerts

Citibank phishing baits customers with fake suspension alerts

By **Bill Toulas** (<https://www.bleepingcomputer.com/author/bill-toulas/>)
February 24, 2022 09:00 AM 0



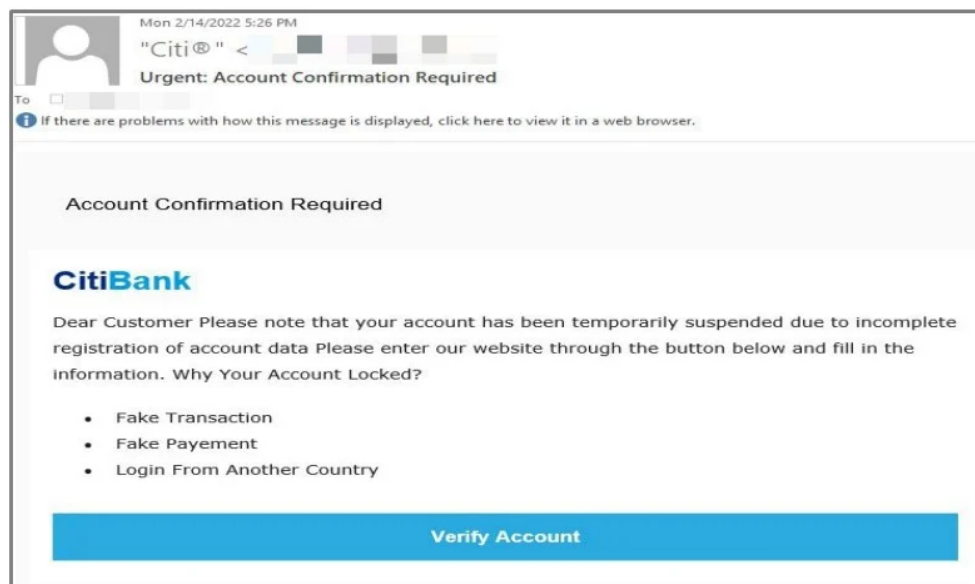


The campaign uses emails that feature CitiBank logos, sender addresses that look genuine at first glance, and content that is free of typos.

The Citibank customers targeted in these attacks are informed that their account has been put on hold due to a suspicious transaction or a login attempt from someone else.



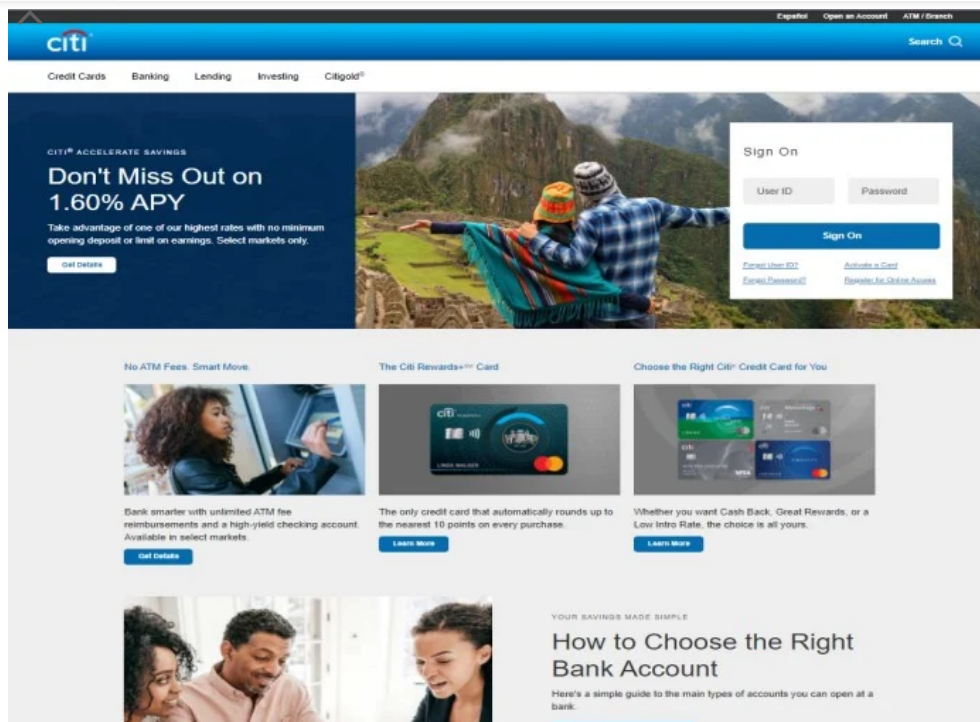
Because of this, the attackers claim they should take urgent action to verify their accounts to avoid permanent suspension.



Sample of the Citibank phishing email (Bitdefender)

If the embedded button is clicked, the victims are taken to a website that looks deceptively like a real Citibank portal, where they are requested to sign in to their online account.





Fake website used for stealing credentials (Bitdefender)

Bitdefender has been tracking this campaign and shared the associated report with BleepingComputer before publication, and reports the following statistical findings:

- 81% of the phishing emails in this campaign target American users
- 7% of the emails reached UK targets, and another 4% ended up in South Korean inboxes
- 40% of these emails were sent from U.S. IP addresses, and 13% from Mexico

A parallel, less convincing effort

Apart from the tactic of creating urgency to cause the recipients to miss obvious signs of fraud and jump into action, phishing actors are also using lures promising enormous winnings.

More specifically, Bitdefender has identified another large-volume phishing campaign whose distribution culminated between February 11 and 15, 2022, presenting the recipients with a chance to claim financial compensation from the United Nations.

The trick employed in this case is to recognize the recipient as a scam victim, one of the 150 who was deemed eligible for a compensation of \$5,000,000 through Citibank.





We removed extra line breaks from this message.

--
Attention beneficiary

This is to bring to your notice that I am delegated from the United Nations to CITIBANK NEW-YORK USA to pay 150 scam victims \$5,000, 000, 00 (\$5 Million US dollar each. You are listed and approved for this payment as one of the scammed victims to be paid this amount, get back to me as soon as possible for the immediate payments of your \$5,000, 000, 00 compensations funds.

I shall feed you with further modalities as soon as I hear from you.
kindly reply to me through this email () so that you can be giving an immediate response.

Yours faithfully,

Executive.

Second campaign phishing email (Bitdefender)

In other cases, the threat actors are doubling the amount to \$10,500,000 and attempt to include more details in the email to convince the victim of its validity.



Mon 2/14/2022 7:55 PM

Citi bank Usa < >

USA International Remittance Department

To

1000 Vermont Ave NW, Washington,
DC 20005, United States
Unclaimed Asset/Assets Re-united,
USA International Remittance Department
E-mail: < >.com
Telephone: +1 206 400 9160
=====

Attn: Beneficiary,

This is to inform you that a compensation payment in the amount of US\$10,500,000.00, (Ten Million five Hundred Thousand United State Dollars) was legally approved and deposited few days ago with our Bank, Citibank Branch Office here in 1000 Vermont Ave NW, Washington, DC 20005, United States and it was deposited in your name by the foreign debts settlement/compensation committee of the Executive Directors Of World Bank Group in conjunction with the European Union Board Of Directors, and they instructed us to credit this fund direct to your private bank account with immediate effect, Meanwhile, the good news about your fund now is that your compensation payment file with some of the legal documents backing this fund has been forwarded to the US Department of State and the United Nations for final approval, And we shall proceed with the transfer immediately we hear from you because we were mandated to transfer this fund to you as one of the beneficiary whose the name is listed in the W orld Bank foreign debts

However, Please note that Citi bank have decided and agreed together to send this payment to you by either bank wire transfer or by ATM/ certified bank draft depending the option you would prefer to receive this fund for security purpose, so you are therefore advised to quickly get back to the management of this bank and let us know the option you choose to have your fund credited into your account to enable us proceed with the claim process of your fund.

We wait your immediate response with your information below to enable this bank proceeds immediately with the transfer of your fund as we were directed.

Full Name.....
Home Address.....
Age/Occupation.....
Valid Phone number.....
Country/State.....
Any Of Your Identity Card.....

Kindly get back to us by reconfirming your full information.
Thank you, God Bless America.
Mr. < >
Director Of Foreign Remittance Department.
Citi bank Usa.

A more outrageous iteration of the same email (Bitdefender)





However, in both cases, the fraud should be pretty obvious, as this is neither how compensations work nor at the level they would be awarded in reality.

For the category of people who believe in these emails, the scammers request them to fill out their full name, address, age, phone number, and a scanned copy of their national ID card.

In this campaign, the details stolen by the victims cannot be directly used for fraudulent transactions but can be instead sold to other criminals on cybercrime markets.

Don't fall for it

Banks rarely ever inform users of important developments on their account via SMS or email, so whenever you receive a message making bold claims, call your bank and ask to speak to an agent.

Do not call phone numbers provided in the email but, instead, visit the bank's official website and source it from the contact page details.

Finally, never click on buttons embedded in the email body and always double-check the URL you are on when preparing to enter login credentials.

