

Trade Now

en every second counts.  
le FX on 4 world-leading platforms  
1 a 99.95% ^ fill rate.

ed on all trades place 1-28 Feb 2022. CFDs are complex instruments and come with a high risk of losing money rapidly due to leverage. 81.12% of retail  
e money when trading CFDs with this provider. You should consider whether you understand how CFDs work, and whether you can afford to take the h  
Refer to our RDN and other legal documents. Pepperstone Markets Limited, SCB no. SIA-F217.

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)  
> Security (<https://www.bleepingcomputer.com/news/security/>)  
> Intuit warns of QuickBooks phishing threatening to suspend accounts

## Intuit warns of QuickBooks phishing threatening to suspend accounts

By **Sergiu Gatlan** (<https://www.bleepingcomputer.com/author/sergiu-gatlan/>)  
May 26, 2022 05:21 PM 0



Tax software vendor Intuit has warned that QuickBooks customers are being targeted in an ongoing series of phishing attacks impersonating the company and trying to lure them with fake account suspension warnings.

Today's alert comes after Intuit received multiple user reports who received these phishing emails and notified their QuickBooks accounts were suspended following a failed business info review.

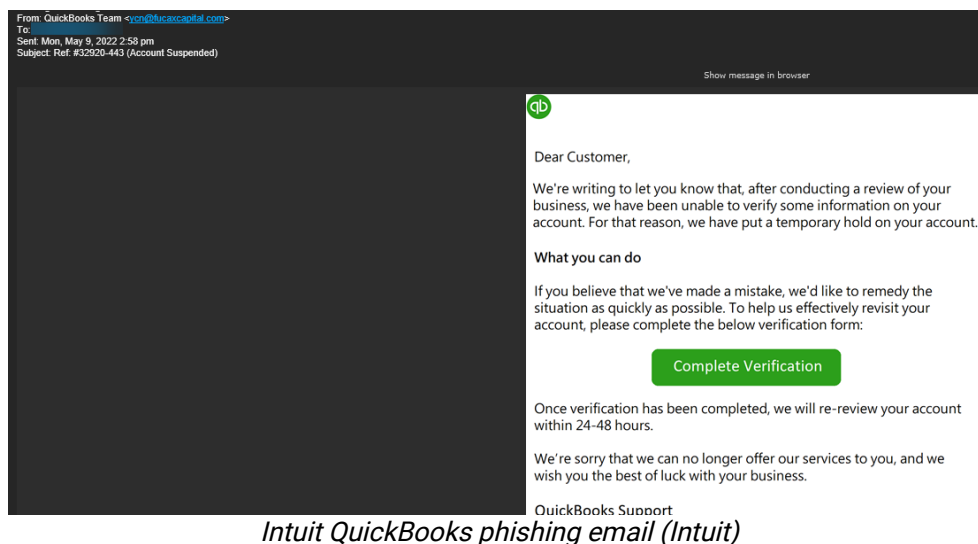
"We're writing to let you know that after conducting a review of your business, we have been unable to verify some information on your account. For that reason, we have put a temporary hold on your account," the attackers say in the phishing messages while impersonating the QuickBooks support team.



"If you believe that we've made a mistake, we'd like to remedy the situation as quickly as possible. To help us effectively revisit your account please complete the below verification form. Once verification has been completed, we will re-review your account within 24-48 hours."

Clicking the "Complete Verification" button in the phishing email will likely redirect the recipients to a landing phishing site designed to harvest their personal information or infect their systems with malware.

The accounting software maker also added that the sender "is not associated with Intuit, is not an authorized agent of Intuit, nor is their use of Intuit's brands authorized by Intuit."



*Intuit QuickBooks phishing email (Intuit)*

## How to make sure you're not phished

Intuit advises customers (<https://security.intuit.com/security-notice#:~:text=Search%20security%20notices-,26%20May%202022,-PHISHING%20EMAIL%3A%20Ref>) who received one of these phishing messages not to click any embedded links or open attachments.

It also recommends deleting them from the inbox to avoid getting infected with malware or sent to some phishing landing page under the attacker's control that would attempt to harvest the targets' credentials.

QuickBooks users who have already opened attachments or clicked links after receiving one of these phishing emails should:

1. Delete any downloaded files immediately.
2. Scan their systems using an up-to-date anti-malware solution.
3. Change their passwords.

Intuit also provides detailed info on how customers can protect themselves from phishing attempts on its support website (<https://security.intuit.com/security-tips>).

Earlier this year, in February, Intuit warned QuickBooks customers (<https://www.bleepingcomputer.com/news/security/intuit-warns-of-phishing-emails-threatening-to-delete-accounts/>) they were the targets of a phishing campaign impersonating the company and threatening to delete their accounts.

In October, threat actors masquerading as Intuit's legal department targeted the company's customers in a fake copyright phishing scam (<https://twitter.com/SlickRockWeb/status/1446494956215017501>) pushing the Hancitor (aka Chanitor) (<https://malpedia.caad.fkie.fraunhofer.de/details/win.hancitor>) malware downloader and Cobalt Strike ([https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt\\_strike](https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike)) beacon.