Intuit warns of phishing emails threatening to delete accounts

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** February 3, 2022 02:22 PM 2

Accounting and tax software provider Intuit has notified customers of an ongoing phishing campaign impersonating the company and trying to lure victims with fake warnings that their accounts have been suspended.

"We have temporarily disabled your account due to inactivity. It is compulsory that you restore your access within next 24 hours," the attackers say in the phishing messages, masquerading as the Intuit Maintenance Team.

"This is a result of recent security upgrade on our server and database, to fight against vulnerability and account theft as we begin the new tax season."

The recipients are instructed to go to https://proconnect.intuit.com/Pro/Update immediately to restore access to their accounts.

Clicking the link will likely redirect them to an attacker-controlled phishing site designed to infect them with malware or harvest their financial or personal information.

Those who might think twice before clicking the embedded link are warned that they might permanently lose access to their accounts.

The financial software maker said that it's not behind these emails and 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."

We have temporarily disabled your account due to inactivity. It is compulsory that you restore your access within next 24 hours.

This is a result of recent security upgrade on our server and database, to fight against vulnerability and account theft as we begin the new tax season.

Please **visit** https://proconnect.intuit.com/Pro/Update to restore your access immediately.

Failure to restore your full access will lead to losing your account permanently

We apologise for any inconvenience this may cause you.

Intuit Maintenance Team,
Intuit Inc.

Sample phishing email (Intuit)

How to avoid getting phished

open attachments.

The recommended way to tackle these phishing attempts is to delete the emails to avoid getting infected with malware or being redirected to a phishing landing page that would try to hand over your credentials.

Customers who already opened attachments or clicked the links in such 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 shares info on how its customers can protect themselves from phishing attacks on its support website (https://security.intuit.com/security-tips).

In October, the company also warned QuickBooks customers of phishing attacks using fake renewal charges as lures (https://www.bleepingcomputer.com/news/security/intuit-warns-quickbooks-customers-of-ongoing-phishing-attacks/).

The same month, QuickBooks users were targeted by scammers via sites threatening them to upgrade to avoid having their databases corrupted or company backup files removed automatically with the end goal of taking over their accounts.

in-turbotax-credential-stuffing-attacks/), and 2021 (https://www.bleepingcomputer.com/news/security/intuit-notifies-customers-of-compromised-turbotax-accounts/).

Related Articles:

FBI warns of fake job postings used to steal money, personal info (https://www.bleepingcomputer.com/news/security/fbi-warns-of-fake-

facebook-accounts-hijacked-via-messenger-phishing/)

Google Drive now warns you of suspicious phishing, malware docs (https://www.bleepingcomputer.com/news/google/google-drive-now-warns-you-of-suspicious-phishing-malware-docs/)

Nintendo warns of spoofed sites pushing fake Switch discounts (https://www.bleepingcomputer.com/news/security/nintendo-warns-of-spoofed-sites-pushing-fake-switch-discounts/)

CISA orders federal agencies to patch actively exploited Windows bug (https://www.bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-patch-actively-exploited-windows-bug/)

INTUIT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/INTUIT/)

PHISHING (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/)

WARNING (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WARNING/)