Protect your QuickBooks Payments account from suspicious activity

7 helpful votes

Get tips in preventing suspicious activity or identity theft in your QuickBooks Payments account.

Suspicious activities and identity theft are growing industry concerns. Follow our guidelines to make sure that your account is safe.

Phishing

Phishing is the act of stealing sensitive info like usernames and passwords by disguising as a trustworthy sender.

Phishing emails

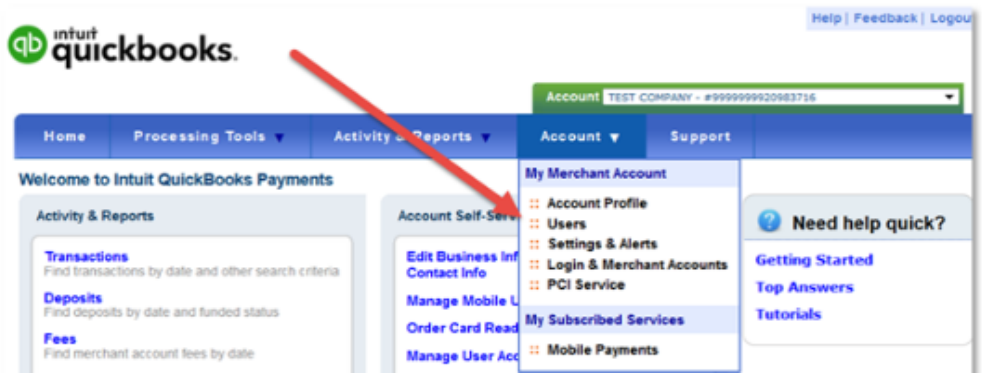
> Important: Intuit or QuickBooks never asks for sensitive info in an email.

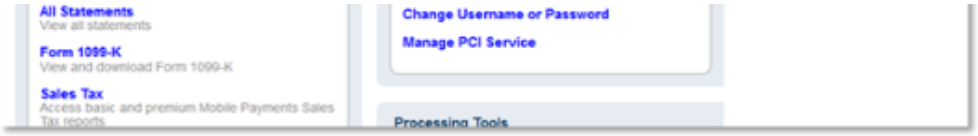
Phishing emails imitate trusted brands and ask you to sign in with your credentials to websites that look real. Make sure that your account is protected. When you receive an email, follow these steps:

1. Ask yourself:
    - Do you recognize the sender's email address?
    - Are there any grammatical or spelling errors in the message?
    - Is the tone consistent with what you would expect from the sender?
    - Is the sender asking you to urgently select a link in the message?
    - Is the sender threatening that you may lose access to your account?
2. Before you open a link in an email, make sure that it's a trusted site like www.quickbooks.com. If it looks suspicious, search the site in your browser. Don't select any links in a suspicious email.
3. Forward the suspicious email to spoof@intuit.com. Don't cut or paste content to keep tracking info. Then, delete the email from your inbox.
4. You can visit our security page for latest security updates on phishing attacks.

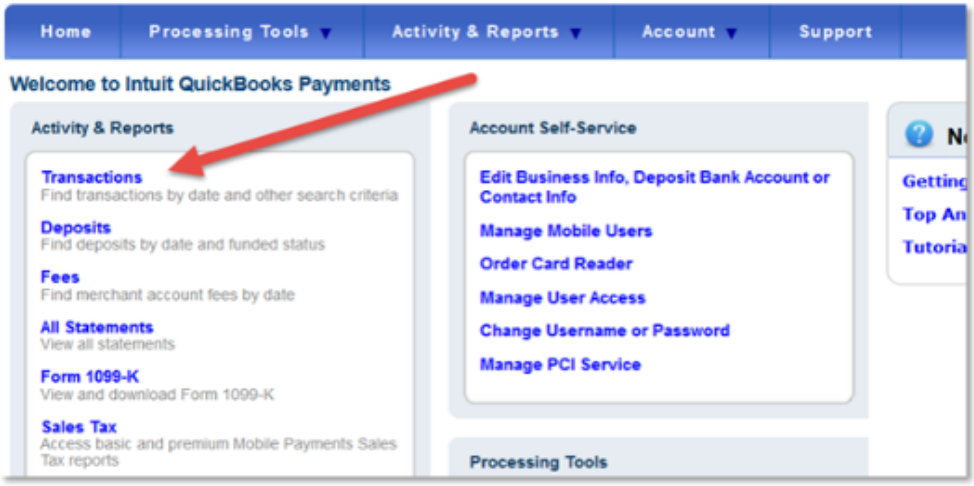
Monitor your account activity

1. Regularly check users that have access to your account in your QuickBooks or the Merchant Service Center website. To see the list of users, select the **Account** tab, then **Users**.





2. In your Activity & Reports, select **Transactions** to check for any transactions that you don't recognize.



3. If there's a bank account change notification that you didn't initiate, call us at 800-397-0707.

Dispute in a QuickBooks Payments Account

> Note: Do not use the search bar of your browser to find our website. Some are suspicious sites that can do harm to your account or computer. You can refer to links that we send in our email or visit our website.

If you think that there will be harm to your QuickBooks Payments account, you need to:

- Call us at 800-397-0707.
- Change the passwords on all your online and email accounts.
- Check if your contact info is updated on all your online accounts. Make sure that there's no unknown phone number or email address.
- Change the passwords on all your online and email accounts.
- Place a fraud alert. Contact the fraud department of the 3 major credit bureaus.
- File a police report. Contact local law enforcement authorities to help us work with your credit agencies.
- Make sure your computer and terminal server was not compromised.
- Monitor your online accounts, account info, and credit report.

Identity theft

When your personal or business info is compromised, they can use that to steal money from your accounts, open new accounts, obtain services, and commit other crimes–all using your personal or business identity.

Account Passwords

To protect your account from any suspicious activity, always use secured account passwords. Here are some tips:

- Use a different password for your email and Intuit account. This ensures that when you confirm any password changes, you are managing two separate passwords.
- Do not share account passwords with others.
- Change your passwords regularly.

A strong password must:

- be more than 8 characters long
- have a combination of lower case, upper case, a number, and a special character like ~!@#$%^&*()_+=?><./
- not contain a word or date associated with you like family names or birth dates
- be a combination of unusual capitalization, numbers, and special characters. Misspelled words are stronger because they're not in the dictionary.
- be something that you can remember
- not be your name, address or phone number
- not be the same with other online accounts

When you report any suspicious activity in your account, our Risk department will investigate the case within a few business days. We will waive all processing fees for transactions that are stolen or fraudulent cards and checks. But, if your personal account was compromised, you could be held financially responsible.