

Phishing Alert for QuickBooks Customers--security plug-in or digital certificate

Overview

IMPORTANT UPDATE FOR QuickBooks Customers: Intuit is receiving reports of individuals receiving fraudulent emails from QuickBooks or QuickBooks Online. The two separate emails ask customers to either download a plug in to assess their security or download a Digital Certificate. Customers should delete either of these emails. As we discover these fraudulent sites (cyber criminals often use the same email repeatedly, although they change web sites), we take them down.

Email texts

The text of the fraudulent emails are below. The first email is about a fake security plug-in.

As is the case with many companies that maintain large databases of information, Intuit is the target of fraudulent attempts to access and extract information from its database. We recently learned our database was illegally accessed and certain contact and personal data were taken, including QuickBooks names, email addresses, phone numbers. The information accessed does not include banking information.

Immediately upon learning about this, Intuit started an investigation and took corrective steps. It is important to know the company continually monitors for any illegal use of information in our database, and so far, we have not detected the misuse of this information.

In order to help assure the security of your information, we have developed a special plug-in for browser and Windows - QuickBooks Update. This software will protect users private information from any kinds of spyware or malware.

System requirements:

- Windows XP, Vista, 2000, 2003
- Internet Explorer 6.x, 7.x, 8.x

ATTENTION: You will not be able to use our service without update from 29 of November 2009

Download:

- Windows QuickBooks Update
- Internet Explorer plug-in

If you are not Microsoft Windows user you can use our services as usual

This is the end of the first fraudulent email.

The second email is about a fake digital certificate and appears exactly as it is sent (mistakes included):

Dear Mr(s).

In order to access Intuit after 20 of December 2009, you must have a valid Digital Certificate installed on your Computer.

Creating and installing your Intuit digital certificate s a quick and automaed process.

Knowing with whom you are communicating, it security on internet operations. only encrypt is not enoug, as it provides no proof of the identity of the sender of the encrypted information. Without special safeguards, you risk being impersonated online. Digital certificates provide an electronic means for Intuit to verify your identity. Used in conjunction with encryption, digital certificates provide a more complete security solution, assuring the identity of all parties participating in a transaction.

The Intuit server has its own digital certificate to assure you that you are actually connecting with Intuit and not with an gyp.

To generate your own Digital Certificate, you need to download Digital Certificate generation tool. For security reasons, download is available only once. Please download Digital Certificate generation tool direct to your Microsoft Windows PC. It is important to

note that: Your Intuit digital certificate will expire after one year. You will be prompted to enter an automatic renewal process 30 days prior to certificate expiration.

System requirements :

Internet Explorer 6.x, 7.x, 8.x

Windows XP, Vista, 2000, 2003

ATTENTION: You will not be able to use our service without update from 20 of December 2009

Download :

Digital Certificate generation tool

If you are not Microsoft Windows user you can use our services as usual

Have more than customers, or want to give your accountant access to your books?

Then Upgrade Today! --

simply log in and click "Upgrade" from your home page.

For faster access, bookmark accounting.quickbooks.com in your browser.

This is the end of the second fraudulent email.

Information

On the Internet, "phishing" refers to criminal activity that attempts to fraudulently obtain sensitive information. ♦ There are several ways a scam artist will try to obtain your social security number, driver's license, credit card information, or bank account information. Here is our QuickBooks Online commitment to you, as well as some steps you can take to make sure your data is safe and secure.

Our commitment to you:

What we won't do

1. We will never send you an email with a "software update" or "software download" attachment.
2. We will never send you an email asking you for login or password information to be sent to us.
3. We will never ask you for your banking information ♦ or credit card information in an email. ♦ We will never ask you for confidential information about your employees in an email.

What we'll do

1. We will provide you with instructions on how to stay current with your Intuit product, and we will provide you with information on how to securely download an update from your computer.
2. If we need you to update your account information, we will request that you do so by logging into your account.

Here's what you can do to protect yourself from a phishing attack:

1. If you suspect you have received a phishing email from Intuit, please forward it immediately to spoofof@intuit.com. ♦ We will look into each reported instance.
2. Make sure you subscribe to an anti-virus software ♦ and keep it ♦ up-to-date.
3. Make sure you have updated your web browser to one that includes anti-phishing security features, such as Internet Explorer 7 or Firefox version 3 or higher
4. Make sure that you keep up to date on the latest releases and patches for your operating systems and critical programs. These releases are frequently security related.
5. Do not respond to emails asking for account, password, banking, or credit card information.
6. Do not open up an attachment that claims to be a software update. ♦ We will not send any software updates via email.
7. Do not respond to text messages or voicemails that ask you to call a number and enter your account number and pin.
8. Make sure you have passwords on your computer and your payroll files.

Here are 3 common methods that phishers use in their emails

1. **Spoofed email address.** Don't reply to unsolicited email and don't open email attachments. It's easy to fake a From or Reply To address, either manually or with spam software, so never assume an email is real by looking at its header. You might be able to spot fake addresses by checking for domain name misspellings, but this isn't foolproof. Some email

- service providers combat the problem of spoofed addresses by using authentication techniques to verify a sender's integrity.
2. **Fake link.** When in doubt, never click on a link in an unsolicited or suspicious email. Scam emails can contain a hidden link to a site that asks you to enter your log on and account information. A clue: if the email threatens you with account closure if you don't log on soon, you could be the target of phishing. You may be able to tell if a link is real by moving your mouse over it and looking at the bottom of your browser to see the hidden Web address - it will look different than the one you see on the surface.
 3. **Forged Website.** If you must visit a financial site, like your bank or credit card company, enter its known address into the browser location field manually. Use a browser with an anti-phishing plug-in or extension, like FireFox version 3 or higher or Internet Explorer 7. These browsers warn you about forged, high-risk sites. Phony Web sites mimic real sites by copying company logos, images, and site designs. Malicious webmasters can also use HTML, Flash or Java Script to mask or change a browser address.

Visit security.intuit.com to get the most up to date information about phishing. Forward suspicious emails to spoofer@intuit.com.

Last updated 01/13/2010