

QuickBooks Scam



ARTICLE 01.25.17 DEAN DORTON

It's no secret that scammers are continuously looking for new ways to reinvent common scams, especially when it comes to phishing emails. Phishing emails are meant to look real, but trick you into clicking a link, providing personal information, or downloading viruses or malware.

Recently the Better Business Bureau learned of a new version of this scam which is circulating quickly. While anyone may receive this email, scammers are specifically targeting small businesses.

According to the Better Business Bureau, here is how the scam works:

You receive an email with the subject line "QuickBooks Support: Change Request." The message is "confirming" that you changed your business name with Intuit, QuickBook's manufacturer. However, you never made such a request. It must be a mistake, but fortunately the email contains a link to cancel.



Pause before you click! Scammers know that you didn't make this request, and the link to cancel is simply bait. It downloads malware to your device, which scammers use to capture passwords or hunt for sensitive information on your machine. This can open you up to identity theft.

How to Spot a Phishing Scam:

Always be wary of expected emails that contains links of attachments. Here are some other ways to spot phishing messages:

- **Check the reply email address.** One easy way to spot an email scam is to look at the reply email. The address should be on a company domain, such as jsmith@company.com.
- **Check the destination of links.** Hover over links to see where they lead. Be sure the link points to the correct domain (www.companyname.com) not a variation, such as companyname.othersite.com or almostcompanyname.com. Scammers can get creative, so look closely.
- **Consider how the organization normally contacts you.** If an organization normally reaches you by mail, be suspicious if you suddenly start receiving emails or text messages without ever opting in to the new communications.
- **Be cautious of generic emails.** Scammers try to cast a wide net by including little or no specific information in their fake emails. Be especially wary of messages you have not subscribed to or companies you have never done business with in the past.
- **Don't believe what you see.** Just because an email looks real, doesn't mean it is. Scammers can fake anything from a company logo to the "Sent" email address.

Source: [Better Business Bureau](#)

When in doubt, if you have a questionable email, it is best to call the source of that email (person or company) to verify that they sent you something you need to open.

If you have concerns regarding your accounting systems or cybersecurity, please contact your Dean Dorton advisor.