Beware of QuickBooks Payment Scams

By Roger Grimes
KnowBe4
January 31, 2022

Many small and mid-sized companies use Intuit's popular QuickBooks program. They usually start out using its easy-to-use base accounting program and then the QuickBooks program aggressively pushes other complimentary features. One of those add-on features is the ability to send customers' invoices via email.

The payee can click on a "Review and pay" button in the email to pay the invoice. It used to be a free, but less mature, feature years ago, but these days, it costs extra. Still, if you are using QuickBooks for your accounting, the ability to generate, send, receive and electronically track invoices all in one place is a pretty easy sell.

Unfortunately, phishing criminals are using QuickBooks' popularity to send business email compromise (BEC) scams. The emails appear as if they are coming from a legitimate vendor using QuickBooks, but if the potential victim takes the bait, the invoice they pay will be to the scammer.

Worse, the payment request can require that the payee use ACH (automated clearing house) method, which requires the payee to input their bank account details. So, if the victim falls for the scam, the criminal now has their bank account information. Not good.

Note: Some other QuickBooks scam warnings will tell you that QuickBooks will never ask for your ACH or banking details. This is not completely true. QuickBooks, the company and its support staff, never will, but QuickBooks email payment requests often do.

Other QuickBooks Scams

Note, I covered a particular type of QuickBooks involved scam above. There are dozens of others, completely unrelated to this type, including:

- Fraudulent calls pretending to be QuickBooks support agents asking you to renew the license
- Fraudulent emails claiming to be QuickBooks' emergency security updates
- Emails about supposed pricing discounts

Conclusion

Millions of people and businesses use QuickBooks to run their business with tons of customers used to receiving and paying QuickBooks-generated email invoices. By attackers sending out QuickBooks phishing emails, there is going to be some percentage of receivers who are likely to fall for the scam. If it is an unexpected QuickBooks-generated email invoice, check the email header to see if it originated from intuit.com or not. Or contact the involved purported vendor using a trusted alternate method to verify before paying. I think we are going to see a lot more QuickBooks scams in the future.