CONVERSATION HIJACKING: A GROWING THREAT IN ACCOUNTS PAYABLE

71% **of organizations were victims of payments fraud attacks and attempts in 2021**

(The Association for Financial Professionals Payments Fraud and Control Survey)

Fraudulent schemes are becoming more sophisticated, and organizations should be aware of the latest threat known as **conversation hijacking.**

Conversation hijacking is a type of targeted email attack in which cybercriminals insert themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts or other sources.
(Barracuda Networks)

Barracuda Networks found that

conversation hijacking grew almost 270% in 2021

While cybercriminals are usually aggressive and hasty, they might display friendly behavior when hijacking a conversation to appear like the person you know and trust. Consider this example of conversation hijacking:

(All identifiable information has been changed to protect the individuals involved in this scenario):

https://www.emailserver.com

From: Scott Moore <SMoore@propertymanagmentinc.com>
Sent: Thursday, October 13, 2022, 11:40 AM
To: Chris Montalli <floors@dgldflooring.com>
Subject: FW: Buckingham: Your invoice 649 from DGLD Flooring

Your check was put into the cue today for payment. This does not tell me the delivery date yet. I will keep you updated. I am guessing 5 business days.

Scott Moore
Property Management Inc.
Executive Director
SMoore@propertymanagementinc.com
C: 854-956-5045

Regular Interaction

From: Chris Montalli <floors@dgldflooring.com>
Sent: Thursday, October 13, 2022, 1:10 PM
To: Scott Moore <SMoore@propertymanagmentinc.com>
Subject: Re: Buckingham: Your invoice 649 from DGLD Flooring

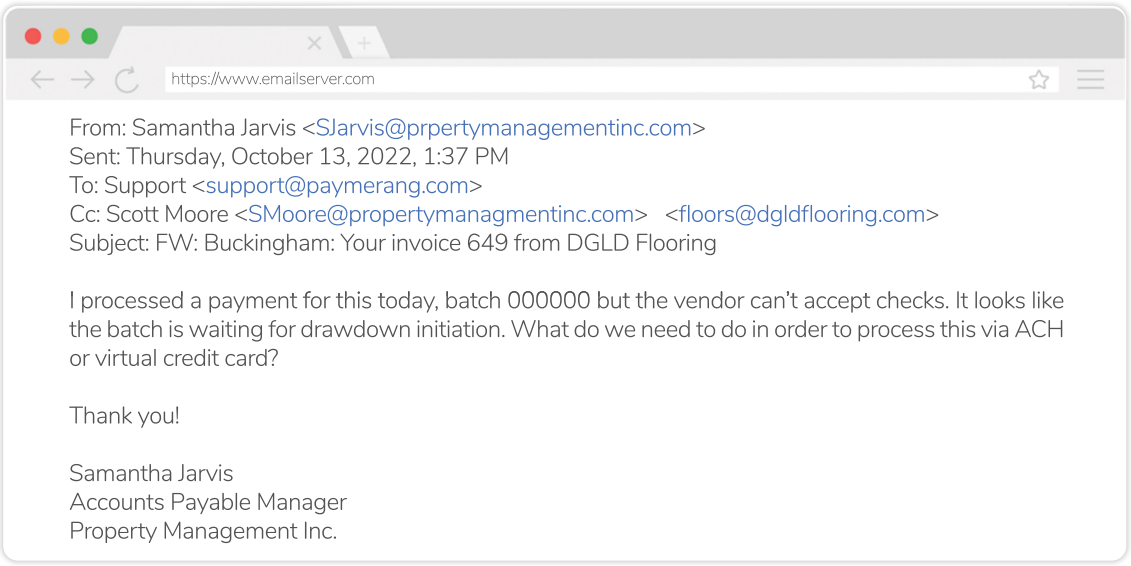
We currently can't process checks right now; we can only accept payment via ACH.

Can you cancel the check and make payment via ACH, what is the information needed to process an ACH payment?

Please confirm.

Chris Montalli
DGLD Flooring
485-985-0265

CONVERSATION HIJACKING: A GROWING THREAT IN ACCOUNTS PAYABLE



From: Paymerang <support@paymerang.com>
Sent: Friday, Oct 14, 2022, at 2:49 PM

Good morning,

Thank you for reaching out to Paymerang. Attached is the ACH enrollment form. Please fill this out with your banking information and we will process the current payment as ACH. Thank you.

Paymerang Steps In

From: <floors@dgldflooring.com>
Sent: Friday, October 14, 2022 at 3:23 PM

See attached ACH filled form, **kindly** acknowledge you receive this and confirm when payment will be initiated. Thank you

DGLD Flooring
Flooring Contractor
485-985-0265
Chris Montalli

Fraud Request Then Takes Place

The example above shows why organizations must always stay vigilant against fraud as it's no longer a matter of *if* but *when* you could become the victim of a fraudulent attack. You must carefully read each email you receive, never provide personal information to a suspicious request, and always check to see if a request is legitimate.

If the company had followed through on this request, it could have cost them thousands of dollars.

$43B

The Federal Bureau of Investigation reported that **between June 2016 and December 2021, there were $43 billion losses from Business Email Compromise.**

Partnering with a best-in-class finance automation provider like Paymerang helps organizations mitigate the risk of fraud. **Schedule a call with our team to learn how!**