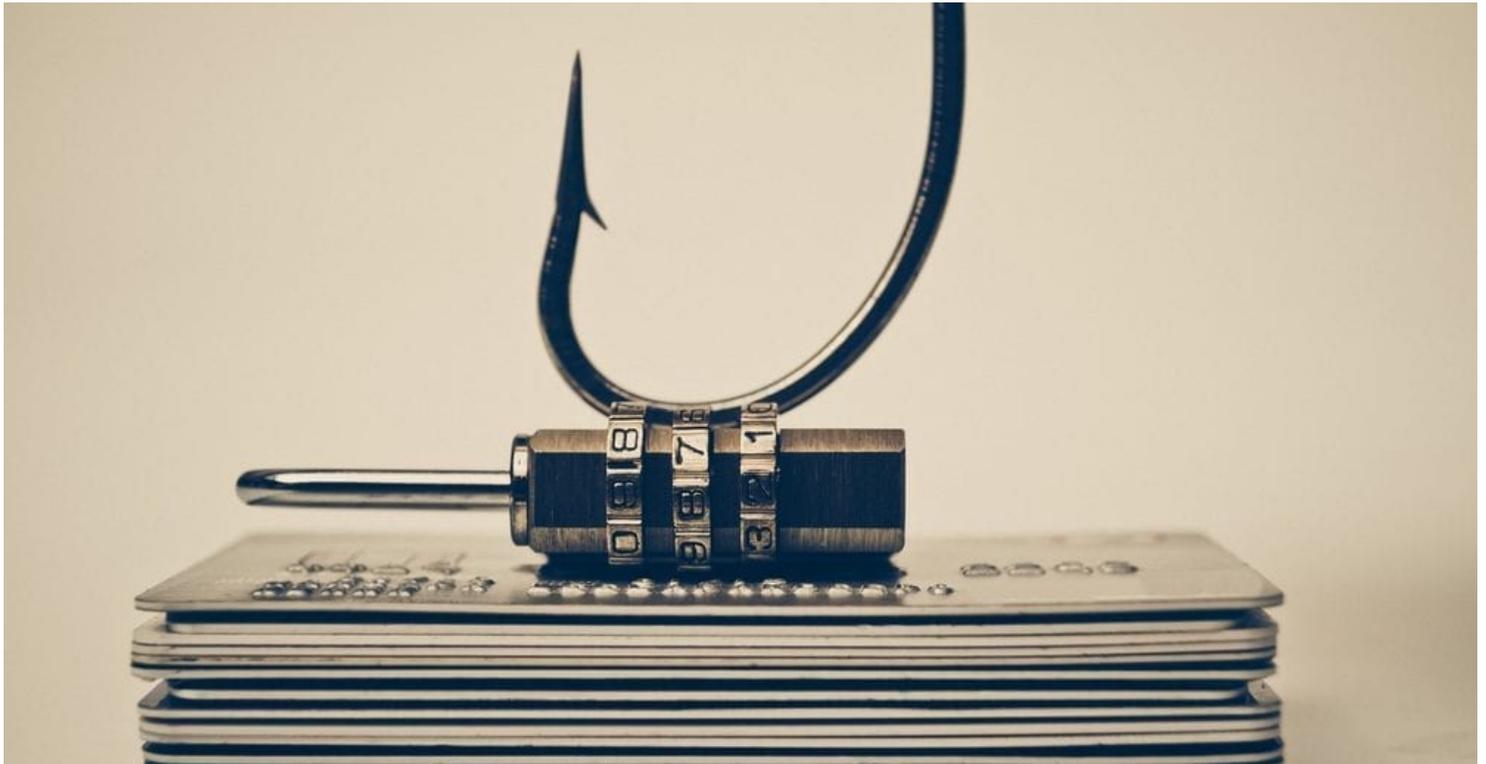


SECURITY & FRAUD

Report: Email Variants Keep BEC Fraud Humming Along

By PYMNTS  

Posted on July 1, 2019



 SHARE  TWEET  SHARE  SHARE  PRINT  EMAIL

In payments fraud, it pays — literally — to change up the game a bit.

As noted in a **report** by FireEye, the bad guys are continuing to leverage a tactic known as business email compromise (BEC), where that method of communication seeks to impersonate persons of authority from within a firm, or alternatively, legitimate business partners, to requests funds be sent to accounts (and then of course, pilfered).

The report shows the use of malicious emails, rather than attachments, is on the rise – which **darkreading.com** said comes along with new variants of impersonation fraud.

The data across a sample set of 1.3 billion emails that spanned the first three months of this year showed there were more URL-based attacks than attachment-based ones.

As reported, the URL attacks are ones that trick recipients with links that bring them to malware or phishing sites. The aim is to steal credentials or credit card data. The way the scammers get past traditional tech defenses is to send largely contentless emails that contain links. There was, the data showed, growth in contentless emails, particularly in the month of January. Here's a variant too: Sometimes the links are "non clickable" and have to be cut and pasted into a browser – whereupon they are activated.

All in all there was a 26 percent quarter-over-quarter boost in malicious emails that sought to bring victims to phishing sites, and in one tactic "spoofed" major brands. That particular variant saw a 17 percent increase as measured in the first quarter. It turns out, according to the report, that Microsoft was the most spoofed brand and accounted for as many as 30 percent of all the malicious URL detections in the first quarter. The roster of other spoofed and well-known brand includes Apple, PayPal and OneDrive, said the report.

Ken Bagnall, vice president of email security at FireEye, said of the report that "the increase in phishing sites using HTTPS was a very interesting shift." In some cases the malicious spoofs aped different Microsoft login pages, prompting the executive to note that "this really highlights how useful attackers see getting access to a victim's Office 365 credentials," Bagnall said.

Individual Fraud Cases, Here and Abroad

Separately, in terms of individual fraud cases, alphanewsmn.com **reported** that in Minnesota, a Blain woman who was charged four years ago with stealing nearly half a million dollars from her former employer (and, the site noted, said her former boyfriend confessed to that crime in a suicide note) has now been accused of stealing \$21,000 from another, subsequent employer.

The site said the accused, Heidi Lynn Meyer, allegedly wrote checks to vendors during her tenure at a flooring and design company. She allegedly wrote 15 checks to vendors that were legitimately owed money, but voided them and deposited them in her own accounts.

Beyond the confines of the U.S., and in the wake of a 2016 disclosure by Brazilian construction firm Odebrecht that it had been involved in a massive bribery scheme, a recent **investigation** by the International Consortium of Investigative Journalists shows that a “cash for contracts” scheme was far more pervasive than had been thought. Among the discoveries via leaked records: More than \$39 million in payments made by the construction firm to coal-fired plant operators in the Dominican Republic, and 17 payments worth more than \$3 million to a Peruvian gas pipeline operator. Secret payments were made to shell companies related to various infrastructure projects, too, said the study.

Latest Insights:

Our data and analytics team has developed a number of creative methodologies and frameworks that measure and benchmark the innovation that’s reshaping the payments and commerce ecosystem. The **July 2019 Pay Advances: The Gig Economy’s New Normal**, a PYMNTS and Mastercard collaboration, examines pay advances – full or partial payments received before an ad hoc job is completed – including how gig workers currently use them and their potential for future adoption.



DOWNLOAD NOW



PYMNTS.com

PAY ADVANCES STUDY

THE GIG ECONOMY'S NEW NORMAL - JULY 2019

RELATED ITEMS: [B2B](#), [B2B PAYMENTS](#), [BEC](#), [EDITORS' PICKS](#), [FIREEYE](#), [FRAUD](#), [NEWS](#), [PAYMENTS FRAUD](#)



SHARE



TWEET



SHARE



SHARE



PRINT



EMAIL



TO TOP