Business Email Compromise (BEC) , Fraud Management & Cybercrime , Fraud Risk Management

FBI: COVID-19-Themed Business Email Compromise Scams Surge

Fraudsters Keep Trying to Turn Pandemic to Their Advantage

Ishita Chigilli Palli (Ishita_CP) • April 7, 2020

Fraudsters are taking advantage of the global COVID-19 pandemic to ramp-up business email compromise scams, the FBI and security researchers warned this week.

See Also: Live Webinar | More Data, More Problems: Applying the Right Automation to Propel Security Operations

In an alert, the FBI says that fraudsters are sending BEC messages that use COVID-19 as an excuse to request a fraudulent switch or rescheduling of payments or a change to other business or government plans in order to pilfer funds.

"Recently, there has been an increase in BEC frauds targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19," according to the FBI.

In one case, FBI agents report that employees at an unnamed financial institution reported receiving an email from someone posing as the firm's CEO and asking to switch a previously scheduled $1 million payment to a different date "due to the Coronavirus outbreak and quarantine processes and precautions."

In another case, a fraudster posing as a client from China sent an email to a business requesting that all invoices be changed to a different bank account due to "Corona Virus audits," according to the FBI. The victim sent several wire transfers to the new account before discovering the fraud.

"Criminals have become more sophisticated by considering the psychological aspects of an attack," says Mark Chaplin, principal at the Information Security Forum. "They anticipate the range of anti-BEC protection likely to be in place and also exploit circumstances relating to individuals receiving the communication. This has resulted in the most skilled, qualified and security-aware employees falling for a well-crafted, targeted attack."

Social Engineering

Over the last month, BEC scammers have begun adjusting their messages to incorporate more concerns over COVID-19 into their social engineering techniques, says Sherrod DeGrippo, senior director of threat research and detection at security firm Proofpoint.

Some fraudsters, for example, are referring to federal government stimulus payments that are being prepared, she points out.

"Cybercriminals know that people and businesses are likely interested in payment information tied to the stimulus package in the U.S., so they are now beginning to send out campaigns around this topic," DeGrippo tells ISMG. "We've seen attempts at email fraud using the idea that the sender is infected and needs the victim to do a task for them or provide some kind of information that they can't obtain themselves due to stay at home orders or sickness."

BEC email using COVID-19 as a lure (Source: Proofpoint)

In one case that Proofpoint researchers recently tracked, BEC scammers used claims of positive COVID-19 cases in one victim's area to start an email conversation, DeGrippo says. The emails, which spoofed real email addresses and names, were sent with "urgent reply" subject lines, but carefully eliminated the possibility of verifying the messages, such as a phone call to confirm the identity of the sender.

"The first email sent is typically innocuous, meaning that they do not contain the attacker's end goal," DeGrippo says. "The attackers craft plausible scenarios in hopes the recipient will reply. Once they're on the hook, the attacker will send their true ask. Those asks then manifest as 'I need you to buy gift cards,' wire transfer funds, etc."

BEC Scams on the Rise

In February, the FBI released its Internet Crime Report, noting that it received nearly 24,000 complaints about BEC scams in 2019, with a total loss of $1.7 billion (see: *FBI: BEC Losses Totaled $1.7 Billion in 2019*).

In March, Palo Alto Network's Unit 42 released its own report that found Nigerian scammers had been ramping up their own BEC schemes in 2019, using much more sophisticated malware and phishing kits to impersonate executives and steal cash from businesses (see: *Nigerian BEC Scammers Increase Proficiency: Report*).

Managing Editor Scott Ferguson contributed to this report.

About the Author

Ishita Chigilli Palli

Senior Correspondent, Global News Desk

As senior correspondent for Information Security Media Group's global news desk, Ishita covers news worldwide. She previously worked at Thomson Reuters, where she specialized in reporting breaking news stories on a variety of topics.