Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

February 16, 2022

Alert Number
I-021622-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise: Virtual Meeting Platforms

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

USING VIRTUAL MEETING PLATFORMS FOR BEC ACTIVITY

Between 2019 through 2021, the FBI IC3 has received an increase of BEC complaints involving the use of virtual meeting platforms to instruct victims to send unauthorized transfers of funds to fraudulent accounts. A virtual meeting platform can be defined as a type of collaboration technique used by individuals around the world to share information via audio, video conferencing, screen sharing and webinars.

Criminals began using virtual meeting platforms to conduct more BEC related scams due to the rise in remote work because of the COVID-19 pandemic, which caused more workplaces and individuals to conduct routine business virtually.

Criminals use virtual meeting platforms to conduct BEC scams in multiple ways:

- Compromising an employer or financial director's email, such as a CEO or CFO, and requesting employees to participate in a virtual meeting platform where the criminal will insert a still picture of the CEO with no audio, or "deep fake[1]" audio, and claim their video/audio is not properly working. They then proceed to instruct employees to initiate transfers of funds via the virtual meeting platform chat or in a follow-up email.
- Compromising employee emails to insert themselves in workplace meetings via virtual meeting platforms to collect information on a business's day-to-day operations.
- Compromising an employer's email, such as the CEO, and sending spoofed emails to employees instructing them to initiate transfers of funds, as the CEO claims to be occupied in a virtual meeting and unable to initiate a transfer of funds via their own computer.

SUGGESTIONS FOR PROTECTION

- Confirm the use of outside virtual meeting platforms not normally utilized in your internal office setting.
- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business/individual it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII of any sort via email. Be aware that many emails requesting your personal information may appear to be legitimate.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.
- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.

If you discover you are the victim of a fraud incident, immediately contact your financial institution to request a recall of funds. Regardless of the amount lost, file a complaint with www.ic3.gov or, for BEC/EAC victims, BEC.ic3.gov, as soon as possible.

[1]Reference Private Industry Notification: PIN Number 210310-001 Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations