Cyber-Enabled Financial Fraud on the Rise Globally

Since 2013, when the FBI began tracking an emerging financial cyber threat called business e-mail compromise (BEC), organized crime groups have targeted large and small companies and organizations in every U.S. state and more than 100 countries around the world—from non-profits and well-known corporations to churches and school systems. Losses are in the billions of dollars and climbing.

At its heart, BEC relies on the oldest trick in the con artist's handbook: deception. But the level of sophistication in this multifaceted global fraud is unprecedented, according to law enforcement officials, and professional businesspeople continue to fall victim to the scheme.

Carried out by transnational criminal organizations that employ lawyers, linguists, hackers, and social engineers, BEC can take a variety of forms. But in just about every case, the scammers target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners—except the money ends up in accounts controlled by the criminals.

> **"BEC is a serious threat on a global scale," said Special Agent Martin Licciardo, a veteran organized crime investigator at the FBI's Washington Field Office. "And the criminal organizations that perpetrate these frauds are continually honing their techniques to exploit unsuspecting victims."**

Those techniques include online ploys such as spear-phishing, social engineering, identity theft, e-mail spoofing, and the use of malware. The perpetrators are so practiced at their craft that the deception is often difficult to uncover until it is too late.

According to the FBI's Internet Crime Complaint Center (IC3), "the BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300 percent increase in identified exposed losses, now totaling over $3 billion."

Although the perpetrators of BEC—also known as CEO impersonation—use a variety of tactics to fool their victims, a common scheme involves the criminal group gaining access to a company's network through a spear-phishing attack and the use of malware. Undetected, they may spend weeks or months studying the organization's vendors, billing systems, and the CEO's style of e-mail communication and even his or her travel schedule.

> **"The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone. Don't rely on e-mail alone."** ***Martin Licciardo, special agent, FBI Washington Field Office***

When the time is right, often when the CEO is away from the office, the scammers send a bogus e-mail from the CEO to a targeted employee in the finance office—a bookkeeper, accountant, controller, or chief financial officer. A request is made for an immediate wire transfer, usually to a trusted vendor. The targeted employee believes he is sending money to a familiar account, just as he has done in the past. But the account numbers are slightly different, and the transfer of what might be tens or hundreds of thousands of dollars ends up in a different account controlled by the criminal group.

If the fraud is not discovered in time, the money is hard to recover, thanks to the criminal group's use of laundering techniques and "money mules" worldwide that drain the funds into other accounts that are difficult to trace.

> **"The ability of these criminal groups to compromise legitimate business e-mail accounts is staggering," Licciardo said. "They are experts at deception. The FBI takes the BEC threat very seriously," he added, "and we are working with our international partners to identify these perpetrators and dismantle their organizations."**

BUSINESS E-MAIL COMPROMISE TIMELINE

An outline of how the business e-mail compromise is executed by some organized crime groups

STEP 1: **Identify a Target**

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

STEP 2: **Grooming**

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

STEP 3: **Exchange of Information**

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

STEP 4: **Wire Transfer**

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

The Art of Deception

The organized criminal groups that engage in business e-mail compromise scams are extremely sophisticated.

Here are some of the online tools they use to target and exploit their victims:

- **Spoofing e-mail accounts and websites:** Slight variations on legitimate addresses (john.kelly@abccompany.com vs. john.kelley@abccompany.com) fool victims into thinking fake accounts are authentic. The criminals then use a spoofing tool to direct e-mail responses to a different account that they control. The victim thinks he is corresponding with his CEO, but that is not the case.
- **Spear-phishing**: Bogus e-mails believed to be from a trusted sender prompt victims to reveal confidential information to the BEC perpetrators.
- **Malware**: Used to infiltrate company networks and gain access to legitimate e-mail threads about billing and invoices. That information is used to make sure the suspicions of an accountant or financial officer aren't raised when a fraudulent wire transfer is requested. Malware also allows criminals undetected access to a victim's data, including passwords and financial account information.

If you or your company have been victimized by a BEC scam, it's important to act quickly. Contact your financial institution immediately and request that they contact the financial institution where the fraudulent transfer was sent. Next, call the FBI, and also file a complaint—regardless of dollar loss—with the FBI's Internet Crime Complaint Center (IC3).

Don't Be a Victim

The business e-mail compromise scam has resulted in companies and organizations losing billions of dollars. But as sophisticated as the fraud is, there is an easy solution to thwart it: face-to-face or voice-to-voice communications.

"The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone," said Special Agent Martin Licciardo. "Don't rely on e-mail alone."

Here are other methods businesses have employed to safeguard against BEC:

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.
- Create an e-mail rule to flag e-mail communications where the "reply" e-mail address is different from the "from" e-mail address shown.
- Color code virtual correspondence so e-mails from employee/internal accounts are one color and e-mails from non-employee/external accounts are another.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having secondary sign-off by company personnel.
- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication; use previously known numbers, not the numbers provided in the e-mail request.
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

Internet Crime Complaint Center

If you believe your business is the recipient of a compromised email or a victim of a BEC scam, file with the Internet Crime Complaint Center (IC3) at www.IC3.gov.

Be descriptive and identify your complaint as "Business Email Compromise" or "BEC."