Frost

PROTECT YOUR BUSINESS

AGAINST BUSINESS EMAIL COMPROMISE (BEC)

BEC is a sophisticated scam targeting businesses that regularly perform wire transfer payments. The scam is not particular in terms of specific business sectors and/or size of the business.

Criminals research organizations, and track key executives (CEOs/CFOs) in order to learn their email styles. Once able to successfully mimic the communication style, a criminal can succeed in reaching and deceiving employees via email. Employees are prompted to wire funds to a fraudulent account, unaware that they are being scammed.

BEC BY THE NUMBERS

$5.3B
from October 2013-December 2016, global BEC scams estimated at $5.3 billion*

$1.5B
from 22,000 U.S. businesses of all sizes from October 2013 to December 2016*

2370%
increase from January 2015-December 2016, 50 states and 131 countries combined*

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 Frost immediately. 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 the email by walking into the requestor's office or speaking to him or her directly on the phone.

* FBI Report: Business Email Compromise, Email Account Compromise–The 5 Billion Dollar Scam, May 4, 2017
**Business Email Compromise: Cyber-Enabled Financial Fraud on the Rise Globally. FBI, Feb. 27, 2017

MITIGATING RISK

Some best practices that can decrease the risk of Business Email Compromise.

Watch for urgent or "secret" requests. Be suspicious of emails that stress the payment needs to be made immediately or if the request is secretive.

Learn to pick up on anything that looks suspicious. Although an email address may look familiar, the recipient should check for letter or character changes that may not be evident at first glance.

Verify with requestor before you send. Be wary of any emailed request instructing a routine wire payment to be sent to a new account.

Create policies that mitigate risk. Employees must confirm authenticity of wire requests by calling the sender at a known or verified phone number. This common practice should be done regardless of urgency, existing relationship, and title (CFO, CEO, etc.) of the requestor.

Test your employees with simulated phishing attacks. Test your employees, share results and potential risks, and train them in order to close the awareness and knowledge gaps.

Change your out-of-office processes. Many BECs take place when key staff members are on vacation. Employees at all levels should refrain from setting an automatic out-of-office email message in order to avoid being impersonated.

(2015 AFP BEC Scams: Treasury's Number One Fraud Threat)

Businesses with awareness and understanding of the BEC scam, and those that implement internal prevention techniques at all levels of the organization can be successful at deflecting BEC attempts.

WE'RE HERE TO HELP

If you see or suspect suspicious activity, please contact Frost's Treasury Management Customer Service Monday through Friday 7am–6pm at 888-481-0336, as well as your local law enforcement.