epcor
Electronic Payments Core of Knowledge
PAYMENTS INSIDER
The inside scoop on payments for businesses of all sizes

The Rise of Business Email Compromise: Protecting Your Business from Costly Scams

by Emily Nelson, AAP, APRP, NCP, Manager, Payments Education, EPCOR

In recent years, business email compromise (BEC) scams have become a significant threat to businesses worldwide. The Federal Bureau of Investigation (FBI) has issued a public service announcement warning about the increasing prevalence of BEC scams, revealing that the total value of redirected funds has exceeded a staggering $12 billion. This article aims to shed light on the evolving nature of BEC scams and their impact on various industries, providing valuable tips to safeguard businesses from falling victim to these costly frauds.

The Growing Scope of BEC Scams

BEC scams have shown no discrimination, targeting businesses of all sizes, personal transactions and even global markets. Reports indicate that these scams have been documented in all 50 states of the United States and across 150 countries worldwide. It is a clear indication that the threat is widespread and affects businesses regardless of their location or scale of operation.

Understanding How BEC Scams Happen

BEC scams can occur in different variations, but they all share the common goal of manipulating victims into transferring funds to fraudulent accounts.

Here are two common versions:

- **Version 1:** Scammers gain access to a legitimate account, often through malware or phishing attacks, and utilize it to conduct unauthorized transfers of funds or direct others within an organization to do so. For example, a fraudster may pose as the CEO and instruct the CFO to wire funds to an account immediately, claiming an urgent need for the transaction. In some cases, scammers create email domains that closely resemble legitimate business addresses to deceive recipients.
- **Version 2:** The fraudster assumes the identity of a legal entity and contacts a business, either through phone calls or emails, regarding an "important matter." Victims are often pressured into wiring money immediately and discreetly.

Tactics and Red Flags

To protect your business from falling victim to BEC scams, it is crucial to be aware of common red flags indicating potentially fraudulent activities. These include:

- Exclusively email-based communication that seems urgent or out of the ordinary.
- Poorly crafted emails, incorrect email signatures or the use of formal language that is atypical for the sender.
- Transactions involving new vendors or contacts.
- Transfer requests made when senior officials are out of the office.
- Large fund transfers to unfamiliar recipients.
- Requests made near the end of the day, weekends or holidays.
- Funds being sent to personal accounts when the company typically only deals with business accounts.
- Receiving accounts with no prior history of large fund transfers.

Protecting Your Business from BEC Scams

Mitigating the risks associated with BEC scams requires a proactive approach and robust security measures. Here are some tips to help safeguard your business:

- Establish a secondary means of communication for verification purposes, especially when dealing with urgent or suspicious requests.
- Implement a policy for identifying and reporting BEC and similar email scams within your organization.
- Exercise caution during phone conversations and avoid disclosing sensitive information.
- Verify any changes in payment type or location mentioned in legal documents before distributing funds.
- Educate your internal staff and key financial officers about the risks and characteristics of BEC scams.

- Implement filters at your email gateway to detect and block emails with known phishing indicators and consider blocking suspicious IP addresses at your firewall.
- In the event of discovering a fraudulent transfer, act swiftly by contacting your financial institution, reporting the incident to your local FBI office and filing a complaint at ic3.gov or bec.ic3.gov.

As the value of funds redirected through BEC scams continues to rise, it is vital for businesses to be proactive in protecting themselves from these fraudulent activities. By understanding the evolving tactics employed by scammers, recognizing red flags and implementing effective security measures, businesses can mitigate the risk of falling victim to BEC scams and safeguard their finances and reputation in an increasingly digital landscape. Stay vigilant and take the necessary steps to protect your business from the costly consequences of BEC scams.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665