Bottomline | PAYMODE

How to Avoid the BEC Iceberg

Statistics stagger us. News reports bring us constant scary updates. Yet, for all the mind-blowing fraud examples, there's reason to believe the true impact of Business Email Compromise (BEC) fraud attempts is understated.

That's because not every incident is reported out of justified fear of reputational damage for the companies affected. In fact, the astonishing reported BEC numbers may be just the tip of the iceberg.

Understanding how BEC works and how to fight it is critical to avoiding the cruel fate of becoming just another statistic.

$55.5 billion in BEC fraud losses over the past decade

The Problem

BEC comes in several flavors, each one deeply unappetizing. Each of these are relatively simple for a fraudster to execute, both at scale and tailored to a particular target, which puts the demanding work on your side.

Spoofs

Fraudsters mimic an existing email address, with a character or two off, and try to get recipients to click on bogus links or surrender information. We've seen the texts from "UPS" and emails from "Amazon," right?

Spearphishing

Targeted, urgent-sounding communications purporting to be from a CEO, attorney, vendor, or other party that tries to create unwise action, such as transferring funds or handing over a password.

Per Fortra, nearly a quarter of emails delivered to corporate inboxes in Q1 2023 were malicious

False Invoice

A fraudster creates a fake invoice, often strikingly real-looking, and sends it via email requesting payment to—you guessed it—the wrong account.

"BEC is the most common and yet one of the most sophisticated types of fraud. If you're not protected against it, your organization is not secure."

— Katie Elliott, Chief Risk & Fraud Officer, Bottomline

The key thread between all types of BEC schemes is that there's sleight of hand. By mimicking a trusted sender's email, a trusted vendor's account, or a fellow employee, a bad actor is hoping to get you to click, send payment, or otherwise take an action you shouldn't. Sometimes that involves an urgent message from your CEO, and sometimes it's a compromised vendor email account requesting you change bank account details. The reason so many organizations fall victim? In a fast-paced, stressful working environment, it's easy not to take a second look.

The Costs

No one knows the full cost because BEC is almost certainly underreported. **Per security firm Arctic Wolf, 70% of businesses were targeted by attempted BEC in the past year,** and some of those hit with successful attacks were able to endure that silently.

$137,000+
is the average cost of successful BEC fraud

$2.7 billion
in average annual BEC losses worldwide

But the numbers that are available make it clear that these cost businesses billions of dollars annually in costs related to the fraud itself, to say nothing of post-incident security hardening and (in many cases) cleanup of reputational damage.

Fortunately, you can take concrete steps to prevent those costs for your own business.

Prevention

Train Employees

Your company should be an environment that fosters critical thinking and prizes security over speed. Conduct regular (read: at least quarterly) training to help employees keep up with trends in BEC fraud and learn to spot obvious fraud, and make sure they know to avoid action, pick up the phone, and/or contact IT if something seems suspicious.

1. Treat requests from senior leaders from vendors with suspicion, especially if they request a check payment, wire transfer or company data or an abnormal payment.

2. Confirm the email's validity with the sender using a different method of contact (OR use an external provider, like Paymode to house the data and offload some of the risk and validation efforts.

3. Use technology that uses artificial intelligence to identify impersonation attempts and malicious patterns in spear phishing emails

Embrace MFA

Multi-factor authentication (MFA) is critical to keep bad actors out of systems, defeating login attempts by forcing a would-be intruder to answer questions and surmount challenges that are unfamiliar. Sending login codes to mobile devices, having multiple challenge questions, and so forth

Implement Email Authentication

Be sure your information technology (IT) team sets up protocols to ensure that incoming emails are from legitimate domains, not illegitimate copies, to filter out many would-be BEC messages.

Protect SIM Cards

For any company phones or personal devices used to access company software and systems, it's best to add a PIN (Personal Identification Number) to your phone's SIM (Subscriber Identity Module) card. This prevents a fraudster from swapping your SIM to their device, allowing them to access any data stored on the card, including messages, contacts, and potentially passwords.

"With the scope of BEC being what it is, you can't possibly fight it alone. Make smart partnerships and seek out proven solutions for your protection and peace of mind." — Katie Elliott, Chief Risk & Fraud Officer, Bottomline

Add Two-Step Verification for Transactions

If you're going to make payments over a certain size, have controls in place to prevent those from being made by a single person who might fall prey to urgent-sounding messages from a fraudster. This can be done with the help of a secure network, but if you're not using one of those, having a layer and/or a second approver can prevent a huge mistake.

Partner Up

Employee vigilance can only go so far, and even layers of do-it-yourself security can't wholly protect you. It's important to partner with firms that can offer monitoring and prevention capabilities that exceed your in-house efforts, shutting down the most sophisticated and hard-to-stop attempts. Scour reviews, source friendly recommendations, and prize experience and track record with any partners you choose.

Don't overlook one more opportunity to partner up, too, to specifically protect your B2B payments from harm.

The Right Business Payment Network Can Make BEC DOA

This iceberg isn't melting. You owe it to yourself to freeze out fraudsters by using a secure payment network.

Secure business payments networks like Bottomline's Paymode hold vendor bank account information and protect your payments behind layers of security and monitoring, ensuring that even if an account is compromised, payments aren't.

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com