BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Business Email Compromise

Tips to protect yourself, and how to respond if you think you have been targeted.

You don't have to work in the finance department of a big company to be the target of business email scams. Business Email Compromise (BEC) is the term for financial cyber events in which the targeted individual is contacted through their work email. The cyber criminal uses a hacked or fake account that looks legitimate in an effort to trick the target into sending funds.

How to Protect Yourself

Be proactive:

- **You are your company's first line of defense.** Know your company's cyber security plan and how to respond to any suspicious emails.
- **Require multiple users to initiate and approve transactions.** If an email looks strange, look up the sender and email or call them (don't use the number they provide).
- **Never trust unknown individuals.** Verify everything they claim and do not send sensitive information to anyone whose identity you can't confirm.
- **Invest in antivirus software** and other cyber security software that can flag suspicious emails and websites.
- **Don't call any numbers,** click on links provided or download attachments from senders until you verify their identity.
- **Escalate if you are at all unsure.** Take the time to discuss your suspicions with your manager or a colleague.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize damage to your business.
- **Contact your bank's servicing desk** or support staff to report a fraulent transaction as soon as you can.
- **Know and follow your local laws** and guidelines for cyber incidents.
- **Document everything** about the event. The more information you have, the better prepared you will be to assist an investigation, and the better prepared you will be against future cyber crime attempts.

The Growing Threat, Measured

23,775

Total number of domestic BEC cases reported to the FBI in 2019.[1]

$1.7 billion

Total adjusted losses in the U.S. in 2019.[1]

1,053

Number of BEC complaints filed between 2018 and mid 2019 using payroll diversion.[2]

[1,2] https://pdf.ic3.gov/2019_IC3Report.pdf

[3] https://www.ic3.gov/media/2019/190910.aspx

Be Cyber-Secure: Business Email Compromise

Why It's Important

Cyber criminals do not discriminate, with targets ranging from wealthy individuals and families to employees at small businesses, nonprofits, school systems and churches. A common threat method is called **phishing,** where seemingly legitimate messages are sent via email or messaging platforms to gain access to systems or data or to install malware (malicious software). This often involves the targeted individual entering sensitive data or clicking on malicious links. There are different types of phishing:

- **Vishing**: a cyber criminal impersonates a trusted source or utilizes tactics such as robocalls, to scam people out of data and money over the phone.
- **Smishing**: utilizes SMS and messaging apps to scam people out of data and money.
- **Spear phishing**: a highly targeted phishing campaign designed for specific individuals.
- **Spoofing:** disguises communications in order to appear to be from someone else, including legitimate businesses or employees. Cyber criminals can spoof emails, phones numbers and websites.

Be alert, business email scams can appear to come from anyone, including:

- **A supplier.** Arrives from a hacked email address to notify you of a bank account change or to request payment.
- **An attorney.** Often arrives during a transaction such as a home purchase, with directions to send an expected payment, like a down payment.
- **A familiar address.** Appears to come from someone you know and asks for confidential information, like payroll records.

Global Information Security at Bank of America

The GIS team is made up of information security professionals staffing multiple security operations centers across the globe who work 24/7 to keep data and information safe.

For more information, go to:
www.bankofamerica.com/privacy/overview.go