U.S. Department of Justice
Federal Bureau of Investigation
Office of Private Sector

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

POTENTIAL TARGETS AND METHODS

- Businesses and personnel using open source email
- Individuals responsible for handling wire transfers within a specific business
- Spoof emails that very closely mimic a legitimate email request (e.g. "Code to admin expenses" or "Urgent wire transfer")
- Fraudulent email requests for a wire transfer are well-worded, specific to the business being victimized

IT & FINANCE SECURITY

- Establish more than one communication channel to verify significant transactions
- Use digital signature on both sides of transactions
- Immediately delete unsolicited email (spam) from unknown parties
- Forward emails and include the correct email address to ensure the intended recipient receives the email
- Remain vigilant of sudden changes in business practices

PROTECTING YOUR ORGANIZATION

- Avoid free web-based email if possible
- Establish a company website domain and use it to establish company email accounts
- Be careful what is posted to social media and company websites
- Be suspicious of requests for secrecy or pressure to take action quickly
- Separate your computer devices from Internet of Things (IoT) devices
- Disable the Universal Plug and Play protocol (UPnP) on your router

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."

CONTACT US: For questions or assistance, locate and contact your local FBI field office at www.fbi.gov