AMERICAN HARDWOOD EXPORT COUNCIL

1825 Michael Faraday Dr.
Reston, VA 20190
Telephone: (703) 435-2900
www.americanhardwood.org

AHEC Trade Alert: Sophisticated Email Scam Affecting US Companies

Please be aware that a sophisticated email scam referred to by the FBI as Business Email Compromise (BEC) has been targeting US businesses making international shipments. This scam occurs when an email is sent from a fake account claiming to be from a US company and requests the wire payment be rerouted to another bank account. Once the wire is sent, this money is not able to be recovered. An AHEC member was recently impersonated using this scam and their customer lost a substantial amount of money. Fortunately this matter has been resolved, but the FBI warns of increasing prevalence of this scam.

In order to prevent this sort of scam from happening to you or your customer, please be cognizant of any red flags during the payment correspondence. If you notice any of the following, proceed with caution.

- non-company standard email address (using @yahoo, @gmail.com, or other generic email when previously you were dealing with someone using an @company-name domain)
- misspelled email address (sometimes using a capital "i" instead of a lowercase "L", etc)
- emails supposedly coming from the US with extremely poor grammar and misspelled words
- suggesting you click on a web link to download invoice, log in, etc
- file attachments that end in .exe or other non document file types (this is a program, **NEVER** open an attachment ending in .exe that someone sends you over email)
- bank information is different than previous orders or the purchase order/contract

Scroll down for guidance from the FBI on how to protect yourself from this sort of online scam. When in doubt, forward the email to someone else at the company you know and confirm the new email address.

To report suspected BEC or other phishing activity, reach out to your local FBI field office at www.fbi.gov.

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