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

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

BUSINESS TRAVEL TIPS

You or your firm may be a target of a foreign country's efforts to obtain information or technologies in order to increase its market share, build its economy, or modernize its military.

Targeting methods include luggage searches, extensive questioning, and unnecessary inspection and downloading of information from laptop computers.

BEFORE YOU TRAVEL

- Obtain specific pre-travel country risk assessments
- Clear personal data or information from your computer, smart phone or other digital device. If you don't need the device, don't take it.
- Make copies of your passport, airplane ticket, driver's license, and credit cards that you take with you. Leave one copy at home
- Establish points of contact for emergencies
- Register your trip with the State Department
- Obtain the phone number and address for the U.S. Embassy or Consulate in the country(s) you plan to visit
- Clean out your voice mail
- Familiarize yourself with local laws and customs in the areas you plan to travel
- Plan your wardrobe so that it does not offend local residents, or draw unwanted attention to yourself
- Do not take unnecessary identification or credit cards

DURING YOUR STAY

- Protect your passport!
- Use authorized taxis
- Do not invite strangers in your room
- Do not carry large amounts of cash
- Do not leave drinks unattended
- Avoid long waits in lobbies and terminals
- Be aware of new acquaintances who probe for information
- Avoid civil disturbances and obey local laws
- Be aware of your surroundings at all times
- Be aware that your conversations may not be private or secure
- Do not leave electronic devices unattended
- Clear your internet browser after each use
- Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American

WHEN YOU RETURN

- Review your system access with your information security officer
- Report any unusual circumstances, including contact by foreigners, to the FBI

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

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

CYBER AWARENESS

Cyber criminals perpetrate a variety of crimes online, including theft of intellectual property, internet fraud, and financial fraud schemes.

Employers and employees can protect themselves by using easy mitigation strategies. Many businesses have dramatically reduced the risk of credential theft and loss of proprietary data.

CYBER BEST PRACTICES

- Use Two-Factor Authentication to increase security by incorporating login requirements with a password along with a token or PIN code
- Ensure your operating system and software are up to date
- Disable hidden file extensions
- Ignore unsolicited emails
- Cover or tape over webcam when not in use
- Use strong passwords
- Disable automatic logins
- Don't leave your computer on 24/7 - turn it off when you're not using it

Electronic Device Tips:

- Understand your Internet of Things (IoT) devices
- Protect your Wi-Fi networks
- Set up firewalls and use complex passwords
- Use media access control address filtering to limit devices that can access your network
- Separate your computer devices from IoT devices
- Disable the Universal Plug and Play protocol "UPnP" on your router

FBI RESOURCES

InfraGard is an information-sharing and analysis effort with private sector partners who own, operate, and hold key positions within 85 percent of the nation's critical infrastructure. It equips its members to identify and mitigate vulnerabilities, develop incident response plans, and enact security best practices. For more details, visit www.infragard.org

CONTACT US: **For questions or assistance, locate and contact your local FBI Field Office at www.fbi.gov**

U.S. Department of Justice
Federal Bureau of Investigation

Office of Private Sector

ECONOMIC ESPIONAGE

Economic Espionage is the act of knowingly targeting or acquiring trade secrets to benefit any foreign government, foreign instrumentality, or foreign agent.

The FBI Field Offices offer counterintelligence training sessions, awareness seminars and other useful information to help industry partners mitigate economic espionage.

KNOW THE SIGNS

- Working odd hours without authorization
- Taking proprietary information home without authorization
- Unnecessarily copying material
- Disregarding company policies on personal software and hardware
- Accessing restricted websites
- Downloading confidential material
- Conducting unauthorized research

PERSONAL BEHAVIORS

- Unexplained short trips to foreign countries
- Engaging in suspicious personal contacts with competitors, business partners or unauthorized individuals
- Buying items they normally cannot afford
- Overwhelmed by life crises or career disappointments
- Showing concern about being investigated

COMMON FACTORS

- Financial need
- Greed
- Unhappiness in the workplace
- Different allegiances to another company or country
- Drug/Alcohol abuse
- Vulnerability to blackmail
- Job offers from other organizations

Targeted Industries or Sectors

- Information and communication technology
- Business information that pertains to supplies of scarce natural resources or that provides global actors an edge in negotiations with U.S. businesses or the U.S. government
- Military technologies (marine systems, unmanned aerial vehicles, and aerospace/aeronautic technologies)
- Civilian and dual-use technologies in fast-growing sectors (clean energy, health care and pharmaceuticals, and agricultural technology)

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

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

ELICITING CORPORATE INFORMATION

Elicitation is a technique used to discreetly collect information that is not publicly available.

KNOW THE SIGNS

- Pretending to have knowledge in common with a person
- Asking a question to which the answer contains at least one presumption
- Building a rapport before soliciting information
- Indicating disbelief or opposition in order to prompt a person to offer information in defense of their position
- Enticing the person to direct a question toward you, in order to set up the rest of the conversation
- Giving information in hopes that a person will reciprocate
- Encouraging a person to expand on what he/she already said

RESPOND EFFECTIVELY

Know what information should not be shared, and be suspicious of people who seek such information. You can politely discourage conversation topics and deflect possible elicitations by:

- Referring them to public sources
- Ignoring any question or statement you think is improper
- Changing the subject
- Deflecting a question with one of your own
- Responding with, "Why do you ask?"
- Giving a nondescript answer

Keep Your Information Safe

Attempts to gather corporate information are usually non-threatening, easy to disguise, deniable, and effective. Do not tell people any detailed information they are not authorized to know. This includes personal information about you, your family, or colleagues.

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

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

PROTECTING INTELLECTUAL PROPERTY

Protect the programs and systems that support what makes your organization successful and unique.

PROTECT YOURSELF AND YOUR COMPANY

- Do not store private information on any device that connects to the internet
- Use up-to-date security software tools
- Educate employees on spear phishing email tactics
- Establish protocols for quarantining suspicious email
- Ensure your employees are trained to avoid un-intended disclosures
- Remind employees of security policies on a regular basis
- Document employee education
- Ensure HR policies are in place that specifically enhance security

Common Hacking Methods

- Malware to your system or download information
- Network hacking
- Theft from unattended electronic devices
- Unauthorized entry
- Unusually probing questions

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

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

SPOTTING INSIDER THREATS

Specialized units in the Federal Government support behaviorally based operational assessments of persons who appear to be on a trajectory toward a catastrophic violent act.

A useful tool to identify, evaluate, and address troubling signs is the creation of a multidisciplinary Threat Assessment Team (TAT) for places of business.

KNOW THE SIGNS

There are some behavioral indicators that should prompt further exploration and attention from law enforcement and/or company officials:

- Development of a personal grievance
- Contextually inappropiate and recent acquisitions of multiple weapons
- Recent escalation in target practice and weapons training
- Recent interest in explosives
- Intense interest or fascination with previous shootings or mass attacks

FBI Support

Threat Assessment Teams may seek assistance from law enforcement that can help assess reported threats or troubling behavior and tap available Federal resources. The FBI's behavioral experts in its National Center for Analysis of Violent Crimes (NCAVC) at Quantico, Virginia are available 24 hours a day, 7 days a week to join in any threat assessment analysis.

CREATE A THREAT ASSESSMENT TEAM

- Review troubling or threatening behavior of persons who display potential indicators
- Include members of the executive leadership or management of the place of business, employees, security personnel, counselors, and medical and mental health professionals connected to the place of business
- Conduct overall analysis of changing behaviors (i.e., behaviors, communication, threats made, security concern, family issues or relationship problems)
- Identify potential victims with whom the individual may interact
- Develop and implement in coordination with other policy and practices for the organization
- Note: a TAT with diverse representation will often operate more efficiently and effectively

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