Business Email Scams: Protecting Your Company's Information

What is Business Email Compromise (BEC)?

Business Email Compromise is a cyber threat targeted against businesses, both large and small, that typically involves a con artist targeting employees with access to company financial or sensitive documents. The scammers lead the employees to believe they are a trusted partner or are legitimately entitled to the information, when in reality, they are criminals.

A common tactic of these cybercriminals is the use of a "spear-phishing" emails and use of malware to first infiltrate the organization and eventually send a sham email supposedly from the CEO to an employee with access to financial information, requesting money to be transferred.

1. Cybercriminal poses as a company exec and emails finance person
2. Finance sends funds to cybercriminal's account
3. Cybercriminal receives the money and disappears

How to protect yourself

- ***Look closely at the email address*** of the person making the request. Scammers often use spoofed emails that look very similar to the legitimate person's account.
  For example: **janeedoe@xyzbusiness.com** versus **janedoe@xyzbusiness.com**.
- ***Never send sensitive information or transfer money*** until you have investigated the request and confirmed, by phone or in person, the request.
- ***Do not use links or phone numbers*** provided in the email request, as these may not be real. Instead, use phone numbers and contact information you know to be correct.
- ***Think before you click*** – do not open attachments or links from unknown senders, or until you have verified the sender of the email. Attachments can install malware onto your computer, allowing cybercriminals to infiltrate the organization.
- ***Work with IT staff*** to flag emails with similar extensions to the organization. For example: the legitimate domain name @xyzbusiness.com could flag fraudulent email domains, such as **@xyz_business.com** or **@xyzbusines.com**.
- ***Implement two-factor or multi-factor authentication*** when sensitive or financial information is involved. For example, require a second staff member to review and approve requests for fund transfers.

Learn more >

Business Email Scams: Protecting Your Company's Information

What to do if you are a victim

- Contact your financial institution immediately and request they contact the financial institution where the transfer was sent
- Contact your local Federal Bureau of Investigation (FBI) field office
  https://www.fbi.gov/contact-us/field-offices
- Contact the Pennsylvania Attorney General, Bureau of Consumer Protection – **1.800-441.2555**
  https://www.attorneygeneral.gov/Complaints/Consumer_Complaint_Form/
- File a complaint with the FBI's Internet Crime Complaint Center (IC3)
  https://www.ic3.gov/default.aspx
- File a complaint with the Federal Trade Commission (FTC) – **1.877.FTC.HELP**
  https://www.ftccomplaintassistant.gov/#crnt&panel1-1
- Contact the Pennsylvania Department of Banking and Securities – **1-800.PA.BANKS**
  http://www.instsearch.pa.gov/Contact.aspx

Cybersecurity Terms to Know

- **Malware** – Short for "malicious software," malware is intended to damage, disable, or perform some other action on a computer or computer system.
- **Spear-phishing** – Spear-phishing is an email scam used to target an individual or organization with the intent to steal data or install malware on the targeted computer or computer system.
- **Spoofing** – Spoofing employs slight changes in an email address or website to fool a victim into thinking the fake email is from a legitimate source.

Connect ··· Learn ··· Contact

pennsylvania
DEPARTMENT OF BANKING
AND SECURITIES

Market Square Plaza | 17 N. Second Street, Suite 1300 | Harrisburg, PA 17101
1.800.PA.BANKS | 1.800.600.0007 | dobs.pa.gov