BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 21-039 **March 2021, Issue #46**

BusinesSafe Threat Topic: Business Email Compromise

Business Email Compromise (BEC) is a cybercrime where scammers use fake email accounts mimicking legitimate businesses or organizations in an attempt to steal money or sensitive information. The scammers typically try to persuade employees to perform a task that goes against normal business practices and may use language in their emails that makes the employee feel a sense of urgency to comply with the scammers demands.

Criminal Activity

BEC involves many techniques to attempt to deceive employees into revealing information or transferring money which may cause serious harm to businesses. A few of the techniques used are:

- **Bogus Invoices** - The scammer will impersonate a supplier either through email, and sometimes even by phone and/or fax, requesting payment for a fake outstanding invoice.
  Toyota Parts Supplier Hit By $37 Million Email Scam

- **Account Compromise** – Scammers compromise an employee's email account and use it to request payments be rerouted to bad actors.
  'Operation Wire Wire': Dozens Arrested in Global Takedown of Business Scammers

- **CEO Fraud** - The scammer will use a compromised email account to send an email to an employee in a company's finance department posing as the CEO or an executive and request a money transfer to a specified account.
  The Exec Email Fraud Menace Continues: Crooks Net $15 Million Via Microsoft's Cloud

- **Data Theft or W2 Attack** - Scammers posing as company management or executives will send an email to specific employees, often those in human resources, requesting personal or identifiable information (such as social security numbers) on employees. This data can be used for future attacks including identity theft.
  HR Professionals: Beware of the Form W-2 Scam

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1, FSIN: 1, 3.1.4, 3.1.7, FFC:1.1, 1.2, 1.3, 1.5, 4.1, 4.3, 4.4

- **Attorney Impersonation** - The scammer will pose as an attorney or law firm representative requesting confidential company information or demanding that a particular matter be handled by the end of the day to avoid further consequences.
  Litigation Over Impostor Email Fraud Mounting in Florida

Ways to Protect Your Business from Business Email Compromise Attacks

- **Use a Company Domain:** Avoid free, web-based email accounts and ensure the business domain is secure.
- **Keep Information Secure:** Be careful about the types of business or employee information that are publicly posted online that could be used for nefarious purposes.
- **Multi-factor Authentication:** Enable multi-factor authentication for all business email and banking accounts and add two levels of authorization for any money transfers.
- **Educate Employees:** Train employees on cyber security, including BEC tactics, and what to look for in emails to spot fraudulent requests.
- **Use Caution when Opening Attachments:** Attachments, especially those sent from unknown senders, are often used to distribute malware. Do not open attachments from unknown parties and if you receive a questionable email alert your supervisor or IT department.

For more information on how to protect your business, you can visit the FBI's website for Business Email Compromise or the Secure Florida's website for Business Email Compromise.

If you believe you have been victimized by a BEC scam, you can:

- File a complaint by calling your local FBI field office or filing online through the FBI Internet Crime Complaint Center.
- If your business has experienced a data breach involving employee information or has received a BEC email requesting employee information you can go to the following IRS website to obtain information on steps to take as well how to report the scam. Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers
- Computer crimes within Florida can also be reported through the Florida Department of Law Enforcement website.

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1, FSIN: 1, 3.1.4, 3.1.7, FFC:1.1, 1.2, 1.3, 1.5, 4.1, 4.3, 4.4