ENER SYSTEMS
INFORMATION TECHNOLOGY SERVICES

Getting rid of unplanned work
*so that others can prosper*

# Disastrous Business Email Schemes And What You Must Do To Reduce The Risk of Compromising The Confidentiality, Integrity And Availability Of Business Information.

**Rene Miller, P.E., CEO Of Ener Systems, Shares One Of Today's Growing Cybersecurity Threats And Must-Dos To Reduce Your Risk.**

It's said that imitation is the greatest form of flattery, but that's **not the case** when it comes to Business Email Compromise (BEC). Email spoofing, is incredibly deceptive because it imitates an email owner's identity and is then used to defraud a company, its employees, its customers, and even partners. Commonly seen attacks will target HR, account receivables & payables, purchasing and a host of other related accounts. These low-life hackers will even use BEC to steal sensitive data, including personally identifiable information (PII). The good news is that with implementation of tools and good practices the risk is reduced.

As CEO of Ener Systems since 1997, a leading technology solutions provider in the Greater New Orleans and North Shore Area, Rene Miller was able to explain the top concerns and questions around BEC attacks

**Q. Are smaller organizations at risk of these types of attacks?**

**Answer:** Yes, small businesses are absolutely at risk. One reason is that small businesses don't always allocate adequate resources to cybersecurity. Operating **without** 2 Factor Authentication on emails, puts every business at high risk of attacks.

**Q. Is there a time of the year when businesses are at a higher risk?**

**Answer:** Actually, yes. We see an uptick in attacks around the major holidays because cyber criminals know the chance of detection is less likely during that time.

**Q. You mentioned 2 Factor Authentication… if a company already has some sort of network security are they covered if a breach happens?**

**Answer:** No. They are at less risk, but every layered security strategy must include something to protect personnel from their own mistakes. At the end of the day, there is always chance of human error. And unfortunately, 80% of victims suffer repeat attacks.

**Q. What should a company do if they find out they have been attacked?**

**Answer:** Act quickly and contact all involved parties! Businesses only have as little as one business day to notify their institution. Next, contact the FBI's Internet Crime Complaint Center.

**Q. Is there something everyone can do right now to help lower the risk?**

**Answer:** End User education and implemented company verification policies are imperative. Adopt 2 Factor Authentication for access to company network and email systems. Also, start implementing these internal methods.

- Confirm requests for transfer of funds
- Have stronger internal controls prohibiting payments initiated by insecure systems such as email
- Require authorized signoff by senior management
- Include a fraud alert statement in the signature line of at-risk emails.
- Color-coded emails with banners for external emails.

No matter the size of your business, layers of cybersecurity are needed in the digital age. Remember, email scammers change their tactics regularly so you must stay vigilant. Start establishing end-user security and provide continual education to employees.

If you have any questions or current security needs, contact Ener Systems through our website or call (985) 871-0333 to schedule a meeting or virtual appointment.

*Annie Vilardo*

*Ener Systems, LLC*