Volume 3, Issue 3

INFRAGARD – NORTH CAROLINA

ncinfragard.org

Inside This Issue

Eastern Carolina President's Update

By: Tim Brown

First, thanks to you "the membership" for making Eastern Carolina InfraGard Member's Alliance (ECI) one of the larger chapters in the country. Your participation in InfraGard is an indication of your concern for our nation's critical infrastructures and the need to protect them from harm and the repercussions of failure should we fail.

Having been involved with ECI since its inception, I have seen this chapter continue to hold the interest of the membership through engaging topics and speakers and other events like the Security Symposium held in Greensboro several years ago. It is my hope that we can continue to hold your interest and engage you more through other activities such as table top exercises. If you have topics of interest or a speaker recommendation, the board would like to hear about them and work on getting the topic covered or have the speaker present at an upcoming meeting. Just remember we depend on donations and sponsorships to fund expenses for the speakers, so we could also use some sponsor suggestions in addition to Cisco who graciously provides their conference space for our regular meetings.

Joining me on the board, until elections are held again in the winter are:

- Sandy Bacik – 1st VP
- Steve Volandt – 2nd VP
- Jim Duncan – Secretary
- John McShane – Treasurer
- Steve McOwen – Law Enforcement Coordinator
- Don Elsner – Outreach and Education Coordinator
- Special Agent Jim Granozio – FBI Board Liaison & InfraGard Coordinator

Sector Chiefs, you know who you are, I think most of you probably feel like you have been in the on deck circle waiting for chance to bat for a couple of years now. Your opportunity to swing the bat is coming. So please make sure we have your up to date contact information.

I look forward to serving as ECI president and hope you can attend an upcoming meeting, if not, please continue take advantage of the InfraGard resources available through the InfraGard portal and alerts provided on the mailing list.

Tim Brown, President Eastern Carolina InfraGard
ncnetsec@gmail.com

CHARLOTTE INFRAGARD CYBERCAMP

Scheduled for July 27-31

We are still looking for sponsors. Interested?

Contact one of the Board Members or click here for more details:
Charlotte Cyber Camp

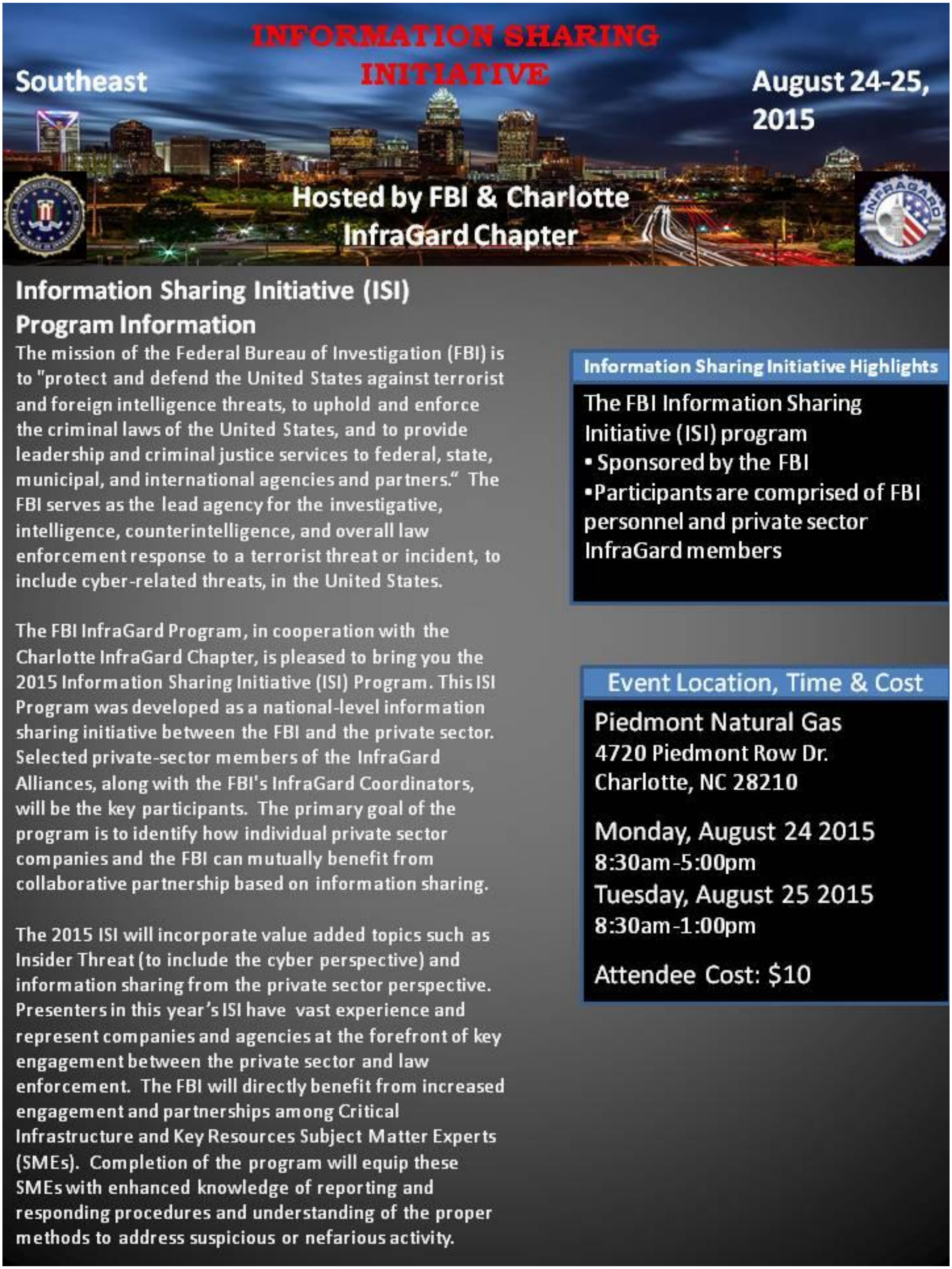
Man–In–the–email scam continues to be a problem – does your financial office know what to look for?

For more than two years, the Internet Crime Complaint Center (IC3) has been receiving complaints from businesses that were contacted fraudulently via legitimate suppliers' e-mail accounts. Recipients were asked to change the wire transfer payment of invoices. Businesses became aware of the scheme after the legitimate supplier delivered the merchandise and requested payment. This scam has been referred to as the "man-in-the-email scam." However, it was recently renamed the "business e-mail compromise."

A twist to this scam that is being reported pertains to the spoofed business e-mail accounts requesting unauthorized wire transfers. In the scheme, a business partner, usually chief technology officers, chief financial officers, or comptrollers, receives an e-mail via their business accounts purportedly from a vendor requesting a wire transfer to a designated bank account. The e-mails are spoofed by adding, removing, or subtly changing characters in the e-mail address that make it difficult to identify the perpetrator's e-mail address from the legitimate address. The scheme is usually not detected until the company's internal fraud detections alert victims to the request or company executives talk to each other to verify the transfer was made. The average dollar loss per victim is approximately $55,000. However, the IC3 has received complaints reporting losses that exceed $800,000.

Recently, the IC3 began receiving related complaints from companies that were alerted by their suppliers about spoofed e-mails received using the company's name to request quotes and/or orders for supplies and goods. These spoofed e-mails were sent to multiple suppliers at the same time. In some cases, the e-mails could be linked by Internet Protocol (IP) address to the original business e-mail compromise scams. Because this latest twist is relatively new, the dollar loss has not been significant. Also, victim companies have a greater chance of discovering the scheme because the e-mails go to multiple suppliers that often follow-up with the company.

Based on analysis of the complaints, the scam appears to be Nigerian-based. Complaints filed contain little information about the perpetrators. However, subject information that was provided has linked to names, telephone numbers, IP addresses and bank accounts reported in previous complaints, which were tied over the years to traditional Nigerian scams.



INFORMATION SHARING INITIATIVE

Southeast

August 24-25, 2015

Hosted by FBI & Charlotte InfraGard Chapter

Information Sharing Initiative (ISI) Program Information

The mission of the Federal Bureau of Investigation (FBI) is to "protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners." The FBI serves as the lead agency for the investigative, intelligence, counterintelligence, and overall law enforcement response to a terrorist threat or incident, to include cyber-related threats, in the United States.

The FBI InfraGard Program, in cooperation with the Charlotte InfraGard Chapter, is pleased to bring you the 2015 Information Sharing Initiative (ISI) Program. This ISI Program was developed as a national-level information sharing initiative between the FBI and the private sector. Selected private-sector members of the InfraGard Alliances, along with the FBI's InfraGard Coordinators, will be the key participants. The primary goal of the program is to identify how individual private sector companies and the FBI can mutually benefit from collaborative partnership based on information sharing.

The 2015 ISI will incorporate value added topics such as Insider Threat (to include the cyber perspective) and information sharing from the private sector perspective. Presenters in this year's ISI have vast experience and represent companies and agencies at the forefront of key engagement between the private sector and law enforcement. The FBI will directly benefit from increased engagement and partnerships among Critical Infrastructure and Key Resources Subject Matter Experts (SMEs). Completion of the program will equip these SMEs with enhanced knowledge of reporting and responding procedures and understanding of the proper methods to address suspicious or nefarious activity.

Information Sharing Initiative Highlights

The FBI Information Sharing Initiative (ISI) program

- Sponsored by the FBI
- Participants are comprised of FBI personnel and private sector InfraGard members

Event Location, Time & Cost

Piedmont Natural Gas
4720 Piedmont Row Dr.
Charlotte, NC 28210

Monday, August 24 2015
8:30am-5:00pm
Tuesday, August 25 2015
8:30am-1:00pm

Attendee Cost: $10

Upcoming Events

Charlotte Chapter Meeting
Date/Time: Wednesday, July 15th from 1-4 pm
Location: Microsoft, 8050 Microsoft Way,
Charlotte, NC.
Register at www.ncinfragard.com

Charlotte Cyber Camp
Dates: July 27-31
Location: Microsoft, 8050 Microsoft Way,
Charlotte, NC.

Eastern Carolina Chapter Meeting
Date/Time: Wednesday, August 19th from 1-4 pm
Location: Cisco, #5, 1025 Kit Creek Rd,
Morrisville, NC.
Register at www.ncinfragard.com

Information Sharing Initiative
Dates: August 24-25
Location: Piedmont Natural Gas, 4720 Piedmont
Row Dr., Charlotte, NC.
Register at www.ncinfragard.com

Charlotte Chapter Meeting
Date/Time: Wednesday, Sept 16th from 1-4pm
Location: Microsoft, 8050 Microsoft Way,
Charlotte, NC.
Register at www.ncinfragard.com

SA James Granozio
InfraGard Coordinator
7915 Microsoft Way
Charlotte, NC 28273
704-672-6351
james.granozio@ic.fbi.gov

InfraGard Helpdesk/Tech Support
(877)861-6298
infragardteam@leo.gov