# Charles H. Eccleston

- Former Department of Energy and Nuclear Regulatory Commission employee
- Age 62 at time of sentencing
- Pled guilty to unauthorized access and intentional damage to U.S. information systems

CDSE

Center for Development of Security Excellence

# CASE STUDY

## Unauthorized Access and Intentional Damage to U.S. Information Systems

### WHAT HAPPENED

On April 15, 2013, Eccleston entered a foreign embassy in Manila, Philippines, and offered to sell a list of over 5,000 e-mail accounts of all officials, engineers, and employees of the U.S. Nuclear Regulatory Commission (NRC). He initially asked for $18,800 to turn over the accounts, stating they were "Top Secret." Eccleston also stated that if his first offer was declined, he would offer the information to China, Iran, or Venezuela, as he believed these countries would be interested in the information.

On November 7, 2013, Eccleston met with FBI undercover employees posing as representatives of an unidentified foreign country and showed them a list of approximately 5,000 e-mail addresses that he said belonged to NRC employees. He offered to sell the information for $23,000. He said the information could be used to insert a virus onto NRC computers that would allow the foreign country to access NRC information or even shut down the NRC's servers. The undercover employee agreed to purchase a thumb drive containing approximately 1,200 e-mail addresses and gave Eccleston $5,000 for the e-mail addresses and $2,000 for travel expenses. It was later determined these e-mail addresses were not classified.

At a follow-up meeting on June 24, 2014, Eccleston was paid another $2,000 and said he had a list of 30,000 e-mail accounts of Department of Energy (DOE) employees. He offered to design and send spear-phishing e-mails that could be used in a cyber-attack on the NRC computer systems.

The undercover FBI agents provided Eccleston with a phony computer virus, and he proceeded to draft spear-phishing e-mails advertising specific nuclear energy conferences. The e-mails were designed to induce the recipients to click on a link that Eccleston believed contained a computer virus that would allow the foreign government to infiltrate or damage the computers of the recipients.

On January 15, 2015, Eccleston sent the spear-phishing e-mails to approximately 80 DOE employees located at various facilities, including laboratories associated with nuclear materials. Eccleston expected to be paid approximately $80,000 for sending the e-mails.

### INDICATORS

- **Foreign Considerations** – Eccleston had frequent contacts with FBI undercover operatives who he thought were representatives of a foreign nation. He also expressed a willingness to sell information to other foreign nations.
- **Technical Activity** – Eccleston used an unauthorized USB device to transfer data from his government laptop to the undercover FBI agents. This is a violation of acceptable user or other automated information system policies.

## IMPACT

- Sentenced to 18 months in federal prison and ordered to forfeit $9,000, an amount equal to the sum the FBI provided to Eccleston during the course of the undercover investigation.
- "Eccleston's sentence holds him accountable for his attempt to compromise, exploit and damage U.S. Government computer systems that contained sensitive nuclear weapon-related information with the intent of allowing foreign nations to gain access to that information or to damage essential systems," said Assistant Attorney General Carlin. "One of our highest priorities in the National Security Division remains protecting our national assets from cyber intrusions. We must continue to evolve and remain vigilant in our efforts and capabilities to confront cyber-enabled threats and aggressively detect, disrupt and deter them."

## ADDITIONAL INFO

- Eccleston was fired from his position as a Facilities Security Specialist at the NRC in October 2010 due to "performance and conduct issues."
- A search of DOE servers confirmed Eccleston sent e-mails to recipients at Oak Ridge National Laboratory in Tennessee, Los Alamos National Laboratory and Sandia National Laboratory in New Mexico, and Lawrence Livermore National Laboratory in California, as well as DOE offices in Washington. D.C.
- On July 30, 2014, Eccleston sent two documents to the FBI undercover agent under a fictitious name. The documents included a table that contained descriptions and links to nine websites for nuclear-related conferences that would occur in the coming year and Eccleston's assessment of the pros and cons of the use of each conference as a lure to target DOE employees in furtherance of the proposed scheme.
- On September 19, 2014, Eccleston sent two more documents to the FBI undercover agents. One of the documents contained two PowerPoint slides advertising an upcoming 2015 conference sponsored by a nuclear society based in Washington, D.C. One of the advertisements included a small yellow rectangle on the lower right hand side of the slide. Inside the rectangle was the following statement: "Conference details and registration: (**Icon to click on**)."

**Questions to consider:**

- What are your organization's "critical assets," and what is your role in protecting them?
- What efforts could be implemented in your organization to enhance awareness of the real dangers associated with phishing attempts?

**Resources for further exploration:**

- Phishing and Social Engineering: Virtual Communication Awareness Training DS-IA103.06 (https://www.cdse.edu/Training/eLearning/DS-IA103/)
- OPSEC Awareness for Military Members, DOD Employees and Contractors GS130.16 (https://www.cdse.edu/Training/eLearning/GS130/)
- Human Resources and Insider Threat Short (https://securityawareness.usalearning.gov/cdse/multimedia/shorts/hrinsider/story.html)

## Supporting Through Reporting

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager