Raising Cybersecurity Awareness at a Small Agency, What Works for Me, Will it Work for You???

Ralph Mosios

Federal Housing Finance Agency

Chief Information Security Officer

March 16, 2016

AGENDA

- Who is FHFA?
- The FHFA Security Awareness Program – Circa 2011
- Transition to the Human Firewall Campaign
- Cybersecurity Newsletters
- The Threat Landscape
- The Social Engineering Experiment
- Social Engineering Results
- How You Can Be Vigilant
- Final Thoughts…

WHO IS THE FEDERAL HOUSING FINANCE AGENCY?

- On July 30, 2008, the Housing and Economic Recovery Act of 2008 (HERA) was enacted, creating FHFA with the combined responsibilities of the Office of Federal Housing Enterprise Oversight, the Federal Housing Finance Board and the HUD Government-Sponsored Enterprises mission team. HERA also provided FHFA with additional authority to regulate Fannie Mae, Freddie Mac and the 12 Federal Home Loan Banks.
- These government-sponsored enterprises provide more than $5.7 trillion in funding for the U.S. mortgage markets and financial institutions.

FHFA DEMOGRAPHICS

- 548 Federal Employees
- 56% Male/44% Female
- Average Age is 48
- 88.7% of employees have a bachelor's degree or higher (59% have advanced degrees).
- FHFA has the second highest percent of advanced degrees.

THE FHFA SECURITY AWARENESS PROGRAM – CIRCA 2011

- New users received general awareness training during employee indoctrination.
- 90% of employees received annual security training.
  - Computer-based training was conducted.
- Users required to re-sign annual rules of behavior.
- No real indication of how effective the program was.

TRANSITION TO THE HUMAN FIREWALL CAMPAIGN

- Distributed monthly cybersecurity newsbytes
  - Non-technical, user friendly articles designed primarily for home use.
- Enhanced Security Intranet site by posting useful links:
  - Fighting Identity Theft - Federal Trade Commission's Consumer Protection Division
  - Consumer and Internet Safety - Federal Trade Commission's Consumer Protection Division
- Educated users to report suspicious email / behavior to the FHFA Help Desk.

CYBERSECURITY NEWSLETTERS

THE THREAT LANDSCAPE

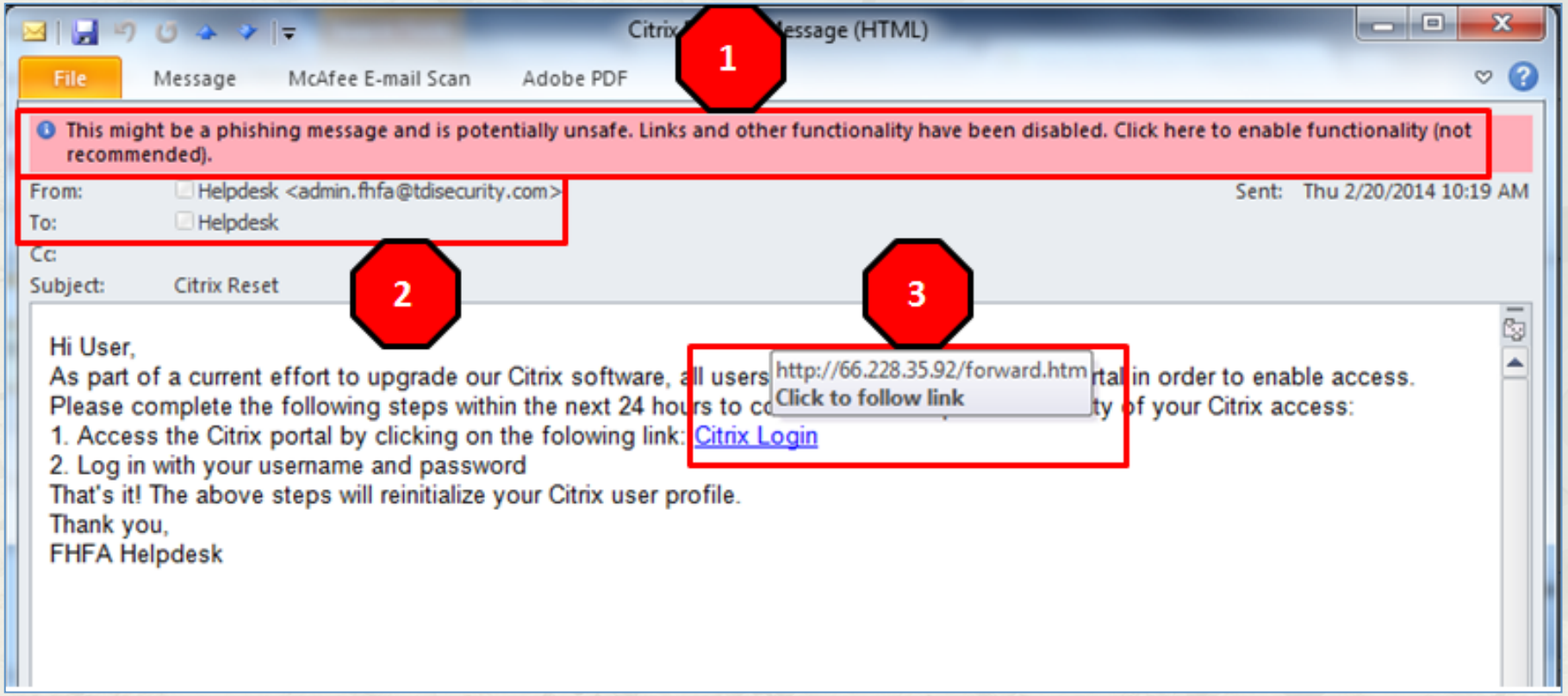
- Sony - Five unreleased movies, an estimated 38 million files of corporate information, and personal information of employees and stars.
- Anthem – 78.8 million records exposed containing customer and employee names, birth dates, Social Security numbers, addresses, email addresses and member IDs.
- Snapchat – Payroll department was targeted by someone impersonating their CEO who asked for employee payroll information.
- Spear phishing attacks continues to be the biggest threat to federal agencies.
  - 91% of cyberattacks begin with spear phishing email [1]

Note: [1] *Email: Most Favored APT Attach Bait,* Trend Micro Research Paper 2012.

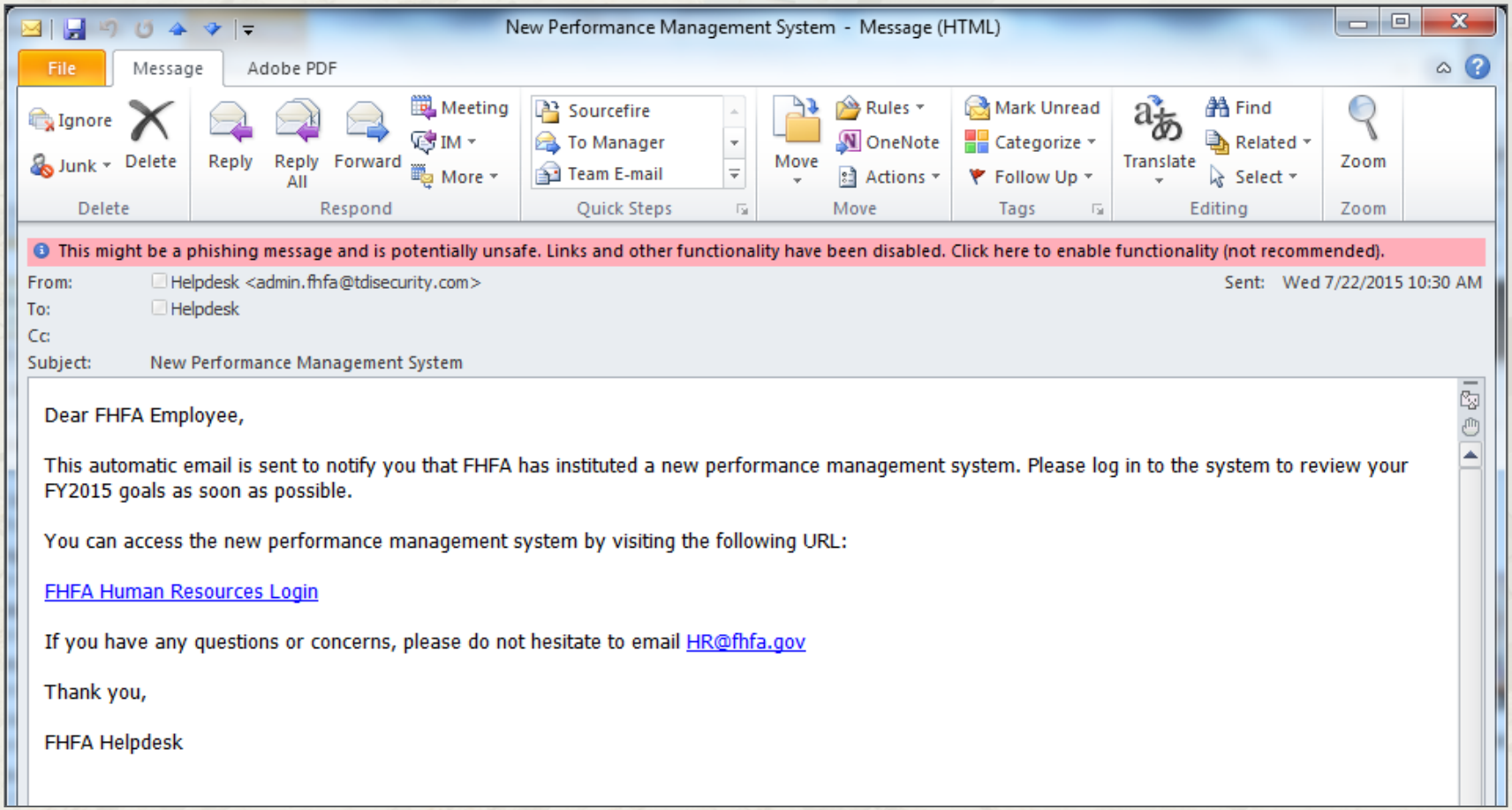
THE SOCIAL ENGINEERING EXPERIMENT

- Security conducted three social engineering tests in three years.
- Phishing emails were sent from outside the FHFA network notifying users to change their passwords and announcing a new Performance Management System.
- USB devices were left on different floors with sample salary data.
- A fake Website was set up to track results.

THE EMAIL - 2014!!!!



THE EMAIL - 2015!!!!



SOCIAL ENGINEERING RESULTS

2012:

- 23 out of 34 users clicked on the embedded link (68%).
- 32% of the users who received this email either deleted it, ignored it, reported it to the Help Desk, or sent emails to IT Security.

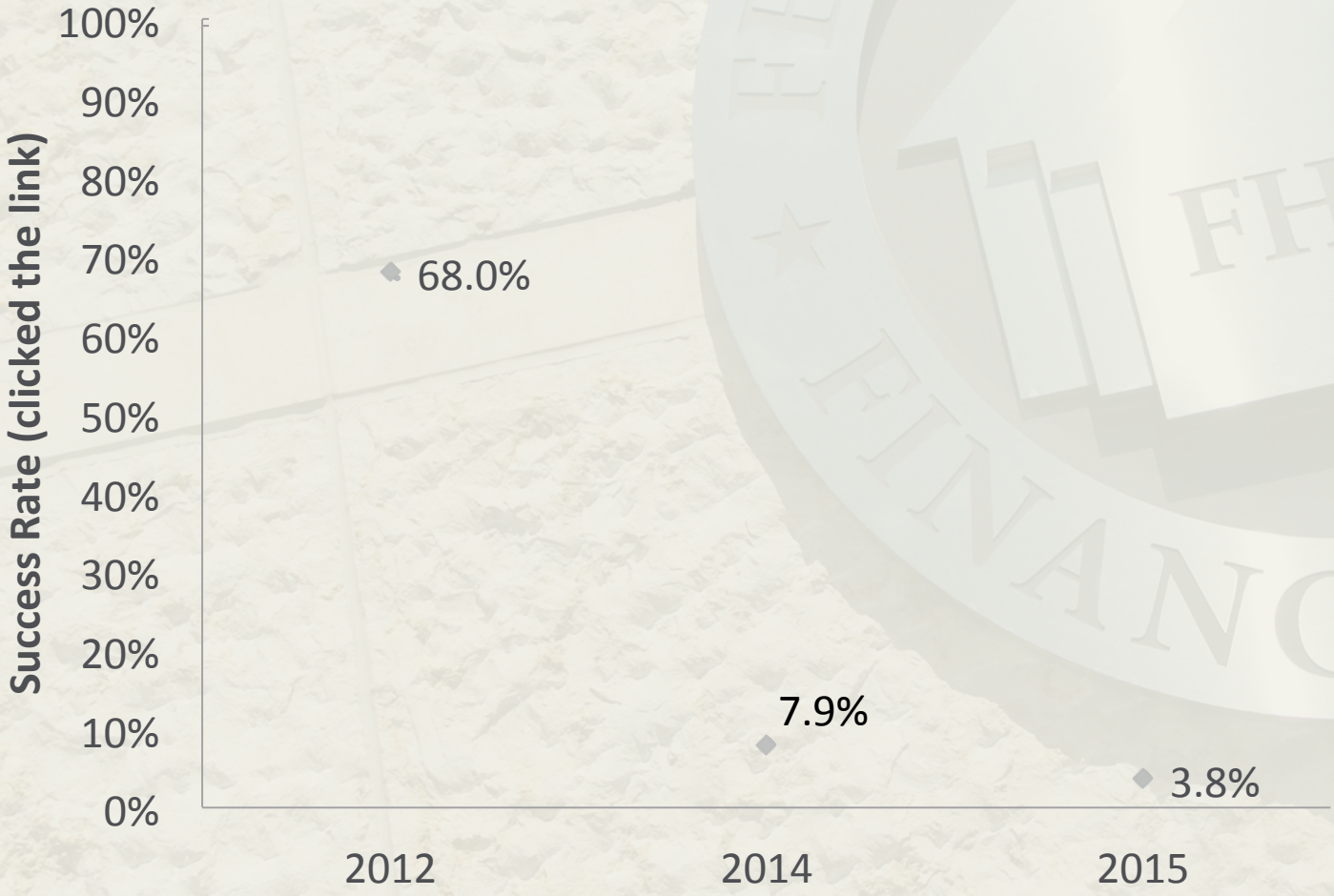
2014:

- 53 out of 668 users clicked the embedded link (7.9%).
- 92.1% of the users who received this email either deleted it, ignored it, reported it to the Help Desk, or sent emails to IT Security.

2015:

- 26 out of 679 users clicked the embedded link (3.8%).
- 96.2% of the users who received this email either deleted it, ignored it, reported it to the Help Desk, or sent emails to IT Security.

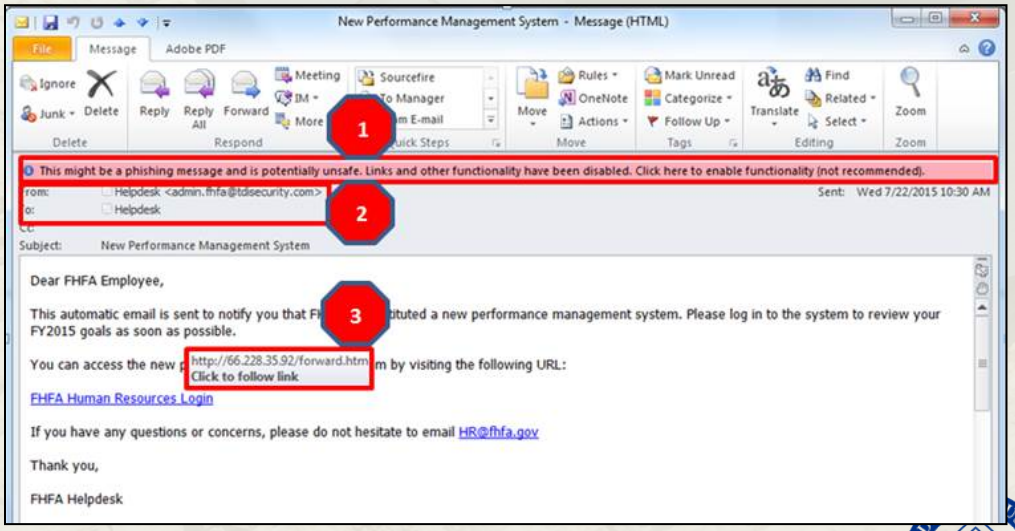
SOCIAL ENGINEERING RESULTS BY YEAR



HOW CAN YOU BE VIGILANT

How to identify potential email phishing attempts:

- Outlook Warning Messages: Outlook will flag suspicious messages. This warning message is a strong indicator of a suspicious message, but is not guaranteed to catch every malicious email.
- Examine the "From" and "To" Address
- Examine Hyperlinks



FINAL THOUGHTS …

- End users are your first line of defense so leverage them.
  - Have them report suspicious activity to the appropriate office.
- Your training approach may require a cultural change.
- Know your audience and tailor your program for your end users.
  - Baby Boomers (1946-1964) vs. Gen X (1965-1979) vs. Millennials (Gen Y; 1980 – 2000) vs. Gen Z (post 2000)
- Raise awareness by using different training techniques.

FINAL THOUGHTS (CONT)…

- Take small steps when necessary.
- Measure your training effectiveness.
- Be proactive and look for different training techniques and mechanisms.
- *Invest in your cybersecurity training program, it's a cost-effective way to protect your network.*

QUESTIONS?????

Ralph Mosios
e-mail: ralph.mosios@fhfa.gov
(202) 649-3680