fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Phishing Panel

Facilitator: Susan Hansche, Department of Homeland Security

Panelists:

Tomm Larson, Idaho National Laboratory

Kimberly Hemby, Center for Medicare and Medicaid Services

Toney Rogers, Health and Human Services

Representative for the U.S. Food and Drug Administration

Homeland
Security

Phishing

The act of tricking individuals into divulging their sensitive information and using it for malicious purposes.

The term “phishing” started in the mid-1990s, but has evolved to encompass a variety of attacks that target personal information.

email is still a vulnerable phishing attack medium…

FY 2019 CIO FISMA Metrics, Version 1 December 2018 (Protect Category)

Security Training and Testing

2.15. Complete the table below to detail the number of users that participated in training exercises to increase awareness and/or measure effectiveness of awareness of phishing in the previous quarter (e.g. agency sends spoofed phishing emails to users and clicking links leading to phishing information page). (OMB M-07-16, NIST SP 800-53r4 AT-2, NIST SP 800-16r1)

https://www.dhs.gov/sites/default/files/publications/FY%202019%20FISMA%20CIO%20Metrics_V1_Final.pdf

FY 2019 CIO FISMA Metrics, Version 1 December 2018

- Number of Users Involved
- Targeted Community
- Summary Of Procedures
- Number of Users Who Successfully Passed the Exercise
- Number of Users that Reported to Appropriate Authority
- Test Date

Targeted Community - Examples

- All Users - All email accounts
- Contractors and Employees
- Targeted components, bureaus, organizations, divisions within the organization
- Users who previously clicked in similar scenario exercises
- New users that had never been phished and users who have failed recent scenarios
- Random Agency Employees, Random 1/3 of all employees
- Privileged users

Summary Of Procedures - Examples

- Training was given on IT system rules of behavior and how to spot phishing emails
- Phish email sent to users, click-throughs recorded, reporting recorded
- Phish email sent, metrics are collected for a minimum of three business days, and up to ten business days, depending on click rate frequency
- Weekly assessment of weekly reported phishes
- Develop monthly phish email, send monthly phish email, send notification and training to users who fail phish
- Report phishing metrics to Directors Office, CIO, CISO, ISSM, and IT Mgrs

Opening Remarks

Tomm Larson
Idaho National Laboratory

Opening Remarks

Kimberly Hemby

Center for Medicare and Medicaid Services

Opening Remarks

Toney Rogers
Health and Human Services

Phishing Awareness Q&A

Tomm Larson: Idaho National Laboratory

Kimberly Hemby, Center for Medicare and Medicaid Services

Toney Rogers: Health and Human Services

Representative for Food and Drug Administration

Panel Contacts

Tomm Larson, INL: tomm.larson@inl.gov

Kimberly Hemby, CMS: Kimberly.Hemby@cms.hhs.gov

Toney Rogers, HHS: toney.rogers@hhs.gov