



Memorandum from the Office of the Inspector General

February 21, 2020

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2019-15621 – TVA NETWORK USER PHISHING AWARENESS

As a part of our annual audit plan, we performed an audit of the Tennessee Valley Authority's (TVA) network user phishing awareness. Our objective was to evaluate the effectiveness of TVA's phishing training provided to TVA network users.

We reviewed the effectiveness of the phishing training provided to TVA users and determined it was ineffective. Additionally, we found TVA does not have formal procedures for conducting periodic phishing exercises, follow-up training for users who failed the periodic exercises, or consequences for users who fail to take required phishing training. Specifics of the identified issues were omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA in a briefing on November 20, 2019.

We recommend the Vice President and Chief Information Officer, Information Technology:

1. Update the content and delivery of end user training to improve phishing awareness.
2. Consider potential consequences for repeat offenders that do not take the required training prior to their assigned deadline.
3. Update procedures to include requirements for periodic phishing exercises, follow-up training, and potential consequences for not taking the required training prior to the deadline.

TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

BACKGROUND

Phishing e-mails are a form of social engineering where an attacker poses as a trustworthy e-mail sender to gain information that can be used to infiltrate an organization's network. According to a 2019 Verizon Data Breach Investigations Report,

32 percent of all breaches in 2019 involved some type of phishing.¹ In 2018, United States Department of Homeland Security reported that phishing e-mails have been used in attacks targeting the energy sector and other control system users.

TVA requires all network users to take cybersecurity awareness training on an annual basis. The training includes informational content on phishing, how to identify it, and what to do if employees receive a phishing e-mail. TVA also purchased a tool to conduct and track periodic phishing exercises to help evaluate the effectiveness of the phishing training. In addition, TVA provides (1) an educational video for users that fail² phishing exercises and enter credentials and (2) a training course for repeat offenders.³

As a part of our annual audit planning, we completed a threat assessment to identify cybersecurity threats that could potentially impact TVA. The potential for a cyberattack utilizing phishing e-mails was one of the areas identified. Therefore, we included an audit of TVA network user phishing awareness as part of our 2019 audit plan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to evaluate the effectiveness of TVA's phishing training provided to TVA network users. The scope of this audit was training related to phishing and did not include technical controls TVA has in place to prevent, detect, and mitigate phishing attempts. The audit scope period was December 12, 2018, to June 28, 2019. We performed fieldwork between December 2018 and November 2019. To achieve our objective we:

- Obtained and reviewed TVA policies.
 - TVA Standard Programs and Processes (SPP) 12.000, *Information Technology*
 - TVA-SPP-12.017, *Security Awareness and Training*
- Obtained and reviewed phishing program related documents provided by TVA Cybersecurity personnel.
- Conducted a walkthrough of TVA's phishing process and tools.
- Obtained and reviewed the results of TVA's phishing exercises.
- Obtained and reviewed industry phishing reports from an established security company that provides phishing services.
- Obtained and reviewed phishing training history provided by TVA personnel.

We did not identify internal controls significant to our audit objective; therefore, internal controls were not tested as part of this audit. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We

¹ "2019 Verizon Data Breach Investigations Report," May 19, 2019, <<https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>>, accessed on December 12, 2019.

² A fail is defined by TVA as a user that clicks on a link in a phishing exercise.

³ A repeat offender is defined as a user that has failed multiple phishing exercises.

believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS

We reviewed the effectiveness of the phishing training provided to TVA users and determined it was ineffective. Additionally, although TVA purchased a tool to conduct and track periodic phishing exercises and requires annual training that includes content on phishing, TVA does not have formal procedures for conducting periodic phishing exercises, follow-up training for users who failed the periodic exercises, or consequences for users who fail to take required phishing training. Specifics of the identified issues were omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA in a briefing on November 20, 2019.

INEFFECTIVE TRAINING FOR USERS THAT FAIL PHISHING EXERCISES

TVA conducted a number of phishing exercises during our audit period (December 12, 2018, to June 28, 2019). These phishing exercises utilized templates provided by a third party phishing tool. We reviewed the results of TVA's phishing exercises and determined that failure rates were consistent with the third party's other customers' failure rates using the same templates. However, we found TVA's repeat offender failure rate was higher than industry average. Higher than average repeat failure rates increase the risk of successful phishing attacks.

TVA established an educational video for users that fail phishing exercises and entered credentials, as well as a training course for repeat offenders. However, we determined TVA's educational video and repeat offender training have been ineffective. Specifically, most users who were provided the educational video closed it before it completed and some users who completed the educational video failed follow-up phishing exercises. In addition, some users who took the required training course for repeat offenders failed subsequent phishing exercises. We also found users were not notified or provided the educational video unless they had entered credentials after clicking on a link.

LACK OF FORMALIZED PROCEDURES ON CONDUCTING PHISHING EXERCISES

TVA has established a phishing program that (1) conducts periodic phishing exercises using a third party tool and (2) requires training for users that fail phishing exercises. We found TVA had documentation of how phishing exercises are conducted, and these exercises were generally conducted in an effective manner. However, we found no formal procedures requiring TVA to conduct periodic phishing exercises or follow-up training for repeat offenders.

In addition, we found most repeat offenders did not take the required training prior to their assigned deadline. Unlike TVA's required annual cybersecurity awareness training, for which failure to complete the annual training results in the individual's network ID being disabled, TVA does not have defined consequences for repeat offenders who do not take the required phishing training by their assigned deadline.

RECOMMENDATIONS

We recommend the Vice President and Chief Information Officer, Information Technology:

1. Update the content and delivery of end user training to improve phishing awareness.
2. Consider potential consequences for repeat offenders that do not take the required training prior to their assigned deadline.
3. Update procedures to include requirements for periodic phishing exercises, follow-up training, and potential consequences for not taking the required training prior to the deadline.

TVA Management's Comments – TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

- - - - -

This report is for your review and management decision. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance. If you have any questions, please contact Weston J. Shepherd, Auditor, at (865) 633-7386 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.



David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

WJS:KDS

cc: TVA Board of Directors
Andrea S. Brackett
Erin L. Cole
Robertson D. Dickens
Melissa A. Livesey
Jeffrey J. Lyash
Justin C. Maierhofer
Jill M. Matthews
Todd E. McCarter
Sherry A. Quirk
John M. Thomas III
OIG File No. 2019-15621

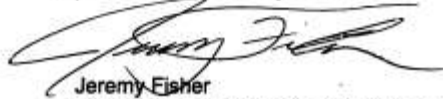
February 14, 2020

David P. Wheeler, WT 2C-K

**RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2019-15621 – TVA
NETWORK USER PHISHING AWARENESS**

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Weston Shepherd, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brandy Brown.



Jeremy Fisher
Vice President and Chief Information Officer
Information Technology
SP 3A-C

ASB:BAB

cc (Attachment): Response to Request

Samuel Austin, MP 3B-C
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Krystal Brandenburg, MP 2B-C
Erin Cole, WT 5D-K
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C

Benjamin Jones, SP 3L-C
Melissa Livesey, WT 5B-K
Jill Matthews, WT 2C-K
Todd McCarter, MP 2C-C
Sherry Quirk, WT 7C-K
John Thomas, MR 6D-C
OIG File No. 2019-15621

Audit 2019-15621
TVA Network User Phishing Awareness
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

	Recommendation	Comments
1	We recommend the Vice President and Chief Information Officer, Information Technology update the content and delivery of end user training to improve phishing awareness.	Management Agrees.
2	We recommend the VP and CIO, IT consider potential consequences for repeat offenders that do not take the required training prior to their assigned deadline.	Management Agrees.
3	We recommend the VP and CIO, IT update procedures to include requirements for periodic phishing exercises, follow-up training, and potential consequences for not taking the required training prior to the deadline.	Management Agrees.