La auditoría de un vistazo

Phishing

ABRIL DE 2021

SOBRE LA AUDITORÍA |
El *phishing* es un tipo de delito informático en el que un agente perverso, que se hace pasar por una persona o empresa legítima, intenta atraer a una persona u organización desprevenida para que comparta información confidencial. La información puede usarse para acceder a sistemas o cuentas importantes, lo que puede resultar en robo de identidad, pérdida de datos y pérdidas financieras.

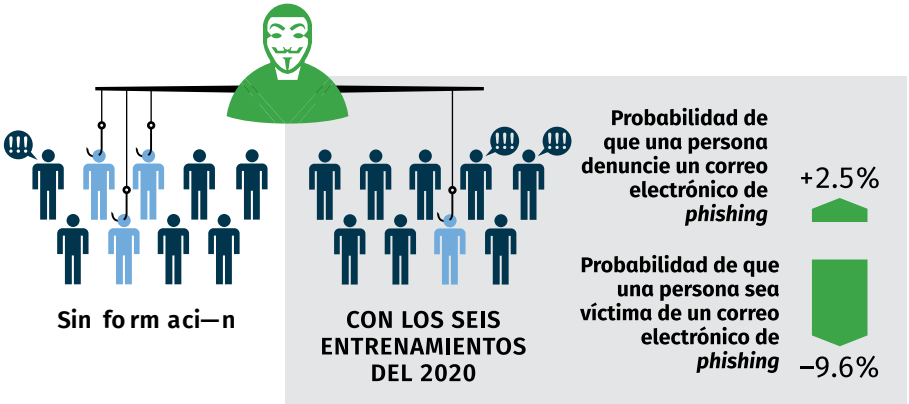
Los *phishing* pueden producirse a través del correo electrónico, de un mensaje de texto o de una llamada telefónica. Los destinatarios pueden ser un público amplio o personas concretas debido a su alto estatus en una organización.

En el reporte

HALLAZGO N.º 1: El Programa de Formación para la Concientización en Ciberseguridad de la ciudad mejora el comportamiento de los empleados hasta cierto punto, pero carece del contenido recomendado y no todos los empleados completan la formación rutinaria

- Se supone que los empleados de la ciudad deben completar la formación en ciberseguridad anualmente para asegurarse de que comprenden los riesgos y cumplen con su función de mantener segura la información de la Ciudad y el Condado de Denver.
- Realizamos un experimento en toda la ciudad para poner a prueba tanto la seguridad organizacional de la ciudad como el comportamiento de los empleados de la ciudad cuando se enfrentan a un correo electrónico de *phishing* simulado. Este correo simulado procedía de un usuario malintencionado que buscaba enviar un programa informático malicioso o recopilar información confidencial.
- Descubrimos que los empleados de la ciudad no cumplen con los estándares recomendados para responder y denunciar correos electrónicos de *phishing*. Sin embargo, también encontramos que la formación en ciberseguridad de la ciudad había generado un efecto positivo pero limitado en los empleados que interactuaron con nuestros correos electrónicos de *phishing* simulados. Por ejemplo, los empleados de la

Cambio en el comportamiento de los empleados después de completar la formación en ciberseguridad



Fuente: *Gráfico diseñado por el personal de la Oficina del Auditor con información de los datos del experimento de phishing de la Oficina del Auditor.*

PASE A LA SIGUIÉNTE PÁGINA →

Timothy M. O'Brien, Contador Público Certificado | Auditor de Denver

CONTINUACIÓN DE LA PÁGINA ANTERIOR

Cronograma de formación

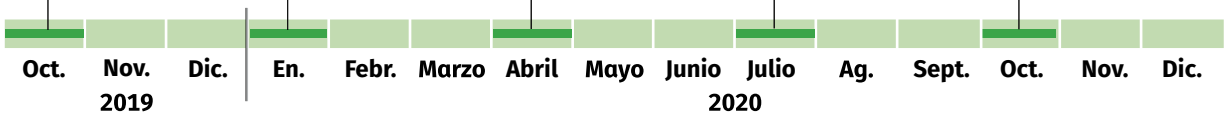
4.º trimestre de 2019
1 de oct. – 31 de oct.
- Fundamentos en seguridad
- Introducción al *phishing*
- Protección contra los programas de chantaje

1.er trimestre de 2020
2 de enero- 21 de enero
- Privacidad de datos

2.º trimestre de 2020
1 de abril - 30 de abril
- Gestión de contraseñas
- Herramientas de protección de correo electrónico
- Reportar una suplantación de identidad

3.er trimestre de 2020
1 de julio - 30 de julio
- Correos electrónicos de *phishing* en la vida real
- Uso ético de los datos

4.º trimestre de 2020
1 de octubre 30 de octubre
- ¿Qué pasa, hijo mío? (Reporte de incidentes)
- ¡No haga clic en eso! Navegación por Internet



Fuente: *Gráfico diseñado por el personal de la Oficina del Auditor utilizando información de los Servicios Tecnológicos.*

ciudad que realizaron todas las formaciones en ciberseguridad requeridas en los primeros tres trimestres de 2020 tenían menos probabilidades, en 9.6 puntos porcentuales, de enviar información confidencial a través de nuestras acciones de suplantación de identidad.

- También evaluamos el contenido del programa de formación en ciberseguridad de la ciudad. Llegamos a la conclusión de que las formaciones no preparan completamente a los empleados para responder a los correos electrónicos de *phishing* ni garantizan que los empleados comprendan el material en su totalidad. Las formaciones más antiguas generaron un menor efecto en el comportamiento, lo que destaca la importancia de realizar formaciones con frecuencia.
- Entre los empleados que interactuaron con nuestros correos electrónicos de *phishing* simulados, se encuentran algunos de los empleados que no están obligados a realizar las formaciones en ciberseguridad de la ciudad. Los empleados que no realizaron las formaciones exponen a la ciudad a un mayor riesgo de pérdida de datos o de infiltración en los sistemas.
- Recomendamos a la ciudad que identifique con mayor precisión los tipos de trabajo de los empleados que deben recibir formación para la concientización en ciberseguridad y que la ciudad evalúe el contenido de la formación para garantizar que se brinde de forma periódica y sea efectiva en la mejora del comportamiento y del conocimiento de los empleados.

HALLAZGO N.º 2: Los servicios tecnológicos deben supervisar las métricas de *phishing* y comunicarlas a otras agencias de la ciudad

- La agencia de Servicios de Tecnología de la ciudad, en colaboración con el Comité de Gobernanza de la Información y la Oficina de Recursos Humanos, es responsable de crear, desarrollar y entregar el contenido del programa de formación en ciberseguridad de la ciudad. Sin embargo, los Servicios de Tecnología no informan formalmente a otras agencias de la ciudad sobre varias métricas relacionadas con los intentos de *phishing*, como la frecuencia con la que los empleados reportan un ataque de *phishing* a los Servicios de Tecnología.
- El personal de Servicios de Tecnología nos dijo que no comunican las métricas de *phishing* a otras agencias de la ciudad, en parte, porque todavía están tratando de recopilar más información para desarrollar las métricas (por ejemplo, información sobre si las mismas personas son víctimas de correos electrónicos de *phishing*).
- Al no comunicar las métricas de *phishing* a otras partes interesadas de la ciudad, es posible que las agencias de la ciudad desconozcan cómo actúan sus agencias y sus empleados cuando ocurren incidentes de *phishing*. Es posible que las agencias tampoco puedan monitorear y supervisar su desempeño para saber si se encuentran por encima o por debajo de las expectativas.
- Recomendamos que los Servicios de Tecnología desarrollen métricas de *phishing* específicas y las comuniquen con otras agencias de la ciudad.