

Laboratorio: Descubra su propio comportamiento riesgoso en línea (versión para el instructor)

Nota para el instructor: El color de fuente rojo o las partes resaltadas en gris indican texto que solamente aparece en la copia del instructor.

Objetivos

Explore las acciones realizadas en línea que pueden comprometer su seguridad o privacidad.

Antecedentes/Escenarios

Internet es un entorno hostil y usted debe estar atento para asegurarse de que sus datos no estén en riesgo. Los atacantes son creativos e intentarán muchas técnicas diferentes para engañar a los usuarios. Esta práctica de laboratorio le permite identificar comportamientos en línea riesgosos y le proporciona sugerencias sobre cómo aumentar su seguridad en línea.

Parte 1: Explore los términos de la política de servicio

Responda las siguientes preguntas con sinceridad y tome nota de los puntos que le corresponden por pregunta. Sume todos los puntos para determinar una puntuación total y continúe con la Parte 2 para realizar un análisis de su comportamiento en línea.

- a. ¿Qué tipo de información comparte con los sitios de redes sociales? _____
 - 1) Todo; dependo de las redes sociales para mantenerme en contacto con mis amigos y familiares. (3 puntos)
 - 2) Artículos o noticias que encuentro o leo (2 puntos)
 - 3) Depende; filtro lo que comparto y con quiénes lo comparto. (1 punto)
 - 4) Nada; no uso redes sociales. (0 puntos)
- b. Cuando crea una cuenta nueva en un servicio en línea: _____
 - 1) Vuelve a usar la misma contraseña que usa en otros servicios para recordarla fácilmente. (3 puntos)
 - 2) Crea una contraseña lo más fácil posible para poder recordarla. (3 puntos)
 - 3) Crea una contraseña muy compleja y la almacena en un servicio de administrador de contraseñas. (1 punto)
 - 4) Crea una contraseña nueva similar a, pero diferente de, una contraseña que usa en otro servicio. (1 punto)
 - 5) Crea una contraseña segura totalmente nueva. (0 puntos)
- c. Cuando recibe un correo electrónico con enlaces a otros sitios: _____
 - 1) No hace clic en el enlace porque nunca sigue los enlaces que le envían por correo electrónico. (0 puntos)
 - 2) Hace clic en los enlaces porque el servidor del correo electrónico ya escaneó el correo electrónico. (3 puntos)
 - 3) Hace clic en todos los enlaces si el correo electrónico es de personas que usted conoce. (2 puntos)
 - 4) Antes de hacer clic, pasa el cursor sobre los enlaces para comprobar la URL de destino. (1 punto)

- d. Cuando visita un sitio web, aparece una ventana emergente. En ella se le indica que su equipo está en riesgo y que debe descargar e instalar un programa de diagnóstico para garantizar su seguridad: _____
- 1) Hace clic en el programa, lo descarga y lo instala para mantener su equipo seguro. (3 puntos)
 - 2) Inspecciona las ventanas emergentes y pasa el cursor sobre el enlace para comprobar su validez. (3 puntos)
 - 3) Ignora el mensaje y se asegura de no hacer clic en este o de no descargar el programa y cierra el sitio web. (0 puntos)
- e. Cuando necesita iniciar sesión en el sitio web de su institución financiera para realizar una tarea: _____
- 1) Ingresa la información de inicio de sesión de inmediato. (3 puntos)
 - 2) Verifica la URL para confirmar que se trata de la institución que buscaba antes de ingresar la información. (0 puntos)
 - 3) No usa servicios financieros o de banca en línea. (0 puntos)
- f. Lee sobre un programa y decide probarlo. Está navegando en Internet y encuentra una versión de prueba de un sitio desconocido: _____
- 1) Rápidamente descarga e instala el programa. (3 puntos)
 - 2) Busca más información sobre el creador del programa antes de descargarlo. (1 puntos)
 - 3) No descarga ni instala el programa. (0 puntos)
- g. Encuentra una unidad USB de camino al trabajo: _____
- 1) Lo recoge y lo conecta a su equipo para mirar el contenido. (3 puntos)
 - 2) Lo recoge y lo conecta a su equipo para borrar por completo el contenido antes de reutilizarlo. (3 puntos)
 - 3) Lo recoge y lo conecta a su equipo para ejecutar un análisis de antivirus antes de reutilizarlo para sus propios archivos (3 puntos)
 - 4) No lo recoge. (0 puntos)
- h. Necesita conectarse a Internet y encuentra una zona de cobertura wifi abierta. Usted: _____
- 1) Se conecta y usa Internet. (3 puntos)
 - 2) No se conecta y espera hasta tener una conexión de confianza. (0 puntos)
 - 3) Se conecta y establece una VPN a un servidor confiable antes de enviar información. (0 puntos)

Parte 2: Analice su comportamiento en línea

Cuanto mayor es su puntuación, menos seguros son sus comportamientos en línea. La meta es ser 100% seguro al prestar atención a todas sus interacciones en línea. Esto es muy importante, dado que solo basta un error para comprometer su equipo y sus datos.

Sume los puntos de la Parte 1. Registre su puntuación. _____

0: usted es muy seguro en línea.

0 – 3: usted es medianamente seguro en línea pero aún debe cambiar su comportamiento para que sea totalmente seguro.

3 – 17: tiene un comportamiento poco seguro en línea y un alto riesgo de ser comprometido.

18 o más: es muy poco seguro en línea y será comprometido.

A continuación, se indican algunas sugerencias de seguridad en línea importantes.

- a. Cuanta más información comparte en las redes sociales, más permite que un atacante lo conozca. Con más conocimientos, un atacante puede diseñar un ataque mucho más dirigido. Por ejemplo, al compartir con el mundo que fue a una carrera de autos, un atacante puede generar un correo electrónico malicioso de la empresa responsable de la venta de entradas para el evento. Dado que usted acaba de asistir a la carrera, el correo electrónico parece más creíble.
- b. Reutilizar contraseñas es una mala práctica. Si reutiliza una contraseña en un servicio bajo el control de los atacantes, probablemente tengan éxito al intentar iniciar sesión como usted en otros servicios.
- c. Los correos electrónicos pueden ser fácilmente falsificados para parecer legítimos. A menudo, los correos electrónicos falsificados contienen enlaces a malware o sitios maliciosos. Como regla general, no haga clic en enlaces incrustados recibidos mediante correo electrónico.
- d. No acepte ningún software no solicitado, especialmente, si proviene de una página web. Es muy improbable que una página web tenga una actualización de software legítima para usted. Le recomendamos que cierre el navegador y que use las herramientas del sistema operativo para consultar las actualizaciones.
- e. Las páginas web maliciosas se pueden desarrollar fácilmente para parecerse a un sitio web de una institución bancaria o financiera. Antes de hacer clic en los enlaces o de proporcionar información, haga doble clic en la URL para asegurarse de estar en la página web correcta.
- f. Cuando permite que un programa se ejecute en su equipo, le otorga mucho poder. Piense bien antes de permitir que un programa se ejecute. Investigue para asegurarse de que la empresa o la persona detrás del programa es un autor serio y legítimo. Además, solo descargue el programa del sitio web oficial de la empresa o de la persona.
- g. Las unidades USB y los dispositivos de memoria incluyen un pequeño controlador que permite que los equipos se comuniquen con ellos. Es posible infectar dicho controlador e indicarle que instale software malicioso en el equipo host. Dado que el malware está alojado en el mismo controlador USB y no en el área de datos, no importa cuántas veces se borre, ningún análisis de antivirus detectará el malware.
- h. Con frecuencia, los atacantes implementan zonas de cobertura wifi falsas para atraer a los usuarios. Dado que el atacante tiene acceso a toda la información intercambiada mediante la zona de cobertura comprometida, los usuarios conectados a dicha zona de cobertura están en riesgo. Nunca use zonas de cobertura wifi desconocidas sin cifrar su tráfico a través de una VPN. Nunca proporcione información confidencial como números de tarjeta de crédito cuando usa una red desconocida (cableada o inalámbrica).

Reflexión

Después de analizar su comportamiento en línea, ¿qué cambios implementaría para protegerse en línea?

Las respuestas pueden variar.