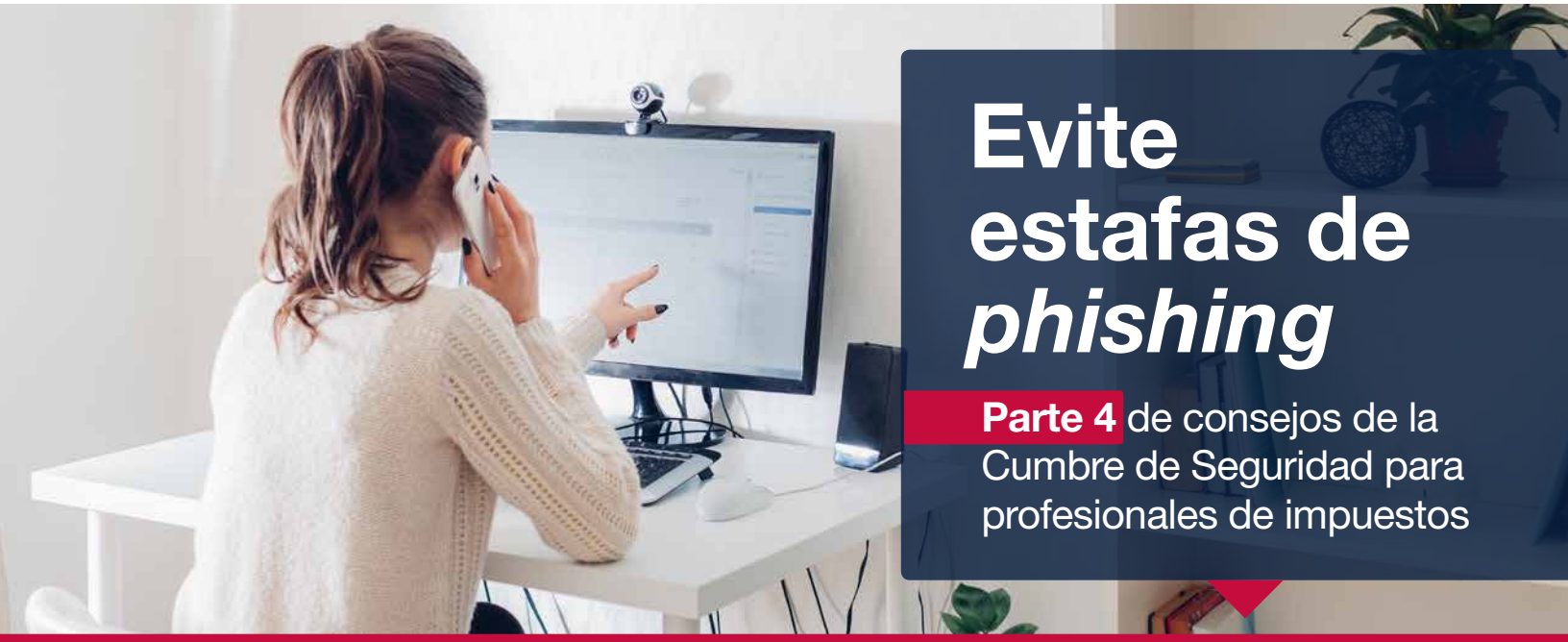
www.irs.gov/cumbredeseguridad

Trabajo virtual: Protección de datos tributarios en el hogar y trabajo

Una serie de cinco partes del IRS y los socios de la Cumbre de Seguridad



Evite estafas de *phishing*

Parte 4 de consejos de la Cumbre de Seguridad para profesionales de impuestos

A medida que los profesionales de impuestos recurren a trabajar desde una ubicación remota, deben estar alertos a estafas de *phishing* por email, especialmente aquellas que se aprovechan de COVID-19 y los pagos de impacto económico. Crear un plan de protección de datos es crítico a medida que los ciberdelincuentes intensifican sus esfuerzos para robar datos tributarios de clientes.

Esto es lo que los profesionales de impuestos deben saber:

- La mayoría de los robos de datos comienza con un truco de correo electrónico de *phishing*.
- Los ladrones de identidad se hacen pasar por fuentes de confianza como un cliente, su proveedor de software o incluso el IRS para provocarlo a abrir un enlace o un archivo adjunto.
- Recuerde, no caiga en la trampa. Aprenda a reconocer y evitar las estafas de *phishing*.
- Cree políticas de “cliente de confianza”; comuníquese con clientes potenciales por teléfono o videoconferencia.

Generalmente, correos electrónicos de *phishing*:

- tienen un mensaje urgente, como que la contraseña de su cuenta venció.
- lo dirige a un enlace o archivo adjunto que parece oficial. El enlace puede llevarle a un sitio falso creado para que parezca una fuente de confianza para robar su nombre de usuario y contraseña.
- o el archivo adjunto puede contener malware, que lo descarga en secreto y permite a los ladrones robar todas las contraseñas del profesional de impuestos.

Los contribuyentes y preparadores de impuestos pueden reportar correos electrónicos sospechosos que dicen ser del IRS a phishing@irs.gov.

Publication 5433-C (SP) (8-2020) Catalog Number 74838S Department of the Treasury **Internal Revenue Service** www.irs.gov