

GRÁFICO EN PANTALLA: Cómo protegerse contra las estafas relacionadas con la COVID-19, Yonesy Núñez, Líder del Grupo de Seguridad de la Información, Wells Fargo, 1 de junio de 2020

GRÁFICO EN PANTALLA: ¿Por qué la protección contra el fraude es especialmente importante ahora?

>> Núñez: La protección contra el fraude es muy importante ahora porque los estafadores se están inclinando a la situación económica de muchos de los norteamericanos, y por eso es muy importante que usted esté atento a estos estafadores.

GRÁFICO EN PANTALLA: ¿Cómo puedo asegurarme de que la comunicación sobre mi cheque de estímulo sea auténtica?

>> Núñez: Para asegurarse de que la información sobre su cheque de estímulo es auténtica, verifique que su correo viene certificado del IRS. El IRS no le mandará información por correo electrónico ni mensaje de texto sobre su cheque de estímulo, sino un correo certificado.

GRÁFICO EN PANTALLA: ¿Cuáles son algunas estrategias populares ahora?

>> Núñez: Las estrategias populares de ahora la que están utilizando los estafadores es enviándoles unos email o mensajes de texto que quieran verificar su información o que usted actualice su contraseña. Tenga mucho cuidado al abrir estos mensajes.

GRÁFICO EN PANTALLA: ¿Cuáles son algunas señales de que un correo electrónico es fraudulento?

>> Núñez: Una de las señales que un correo electrónico es fraudulento es cuando estos quieren que usted verifique su información, le dé un clic a un archivo adjunto o que actualice su contraseña. Los bancos y otras organizaciones nunca le pedirán que usted haga esto por un email.

GRÁFICO EN PANTALLA: ¿Cuáles son algunas señales de una estafa por mensaje de texto?

>> Núñez: Una de las señales de una estafa por mensajes de texto es que le manden un mensaje de texto que quiera verificar su información para usted haciéndole un clic a uno de los enlaces adjuntos. No le haga clic y comuníquese con su organización bancaria o de otra índole para verificar esa información con información que ya usted tiene sobre esta organización, como su factura.

GRÁFICO EN PANTALLA: He visto publicaciones en las redes sociales con ofertas especiales de préstamos. ¿Puedo confiar en ellas?

>> Núñez: Debe de tener mucho cuidado cuando vea una oferta de préstamos de crédito en las redes sociales. Comuníquese directamente con el banco o la compañía financiera para obtener algunos de estas ofertas, no con los clic de enlaces adjuntos en las redes sociales.

GRÁFICO EN PANTALLA: ¿Qué sucede con las comunicaciones que digan ser del IRS o de mi banco?

>> Núñez: Si recibe una comunicación que diga ser de IRS o de su banco por correo electrónico o mensaje de texto para que usted actualice su información personal o de cuenta o de contraseña, su banco ni el IRS nunca le pedirán que actualice esa información por correo electrónico ni mensaje de texto. Verifique directamente llamando a su banco o al IRS.

GRÁFICO EN PANTALLA: ¿Cómo puedo protegerla del fraude?

>> Núñez: Si usted dirige una pequeña empresa, para protegerla del fraude puede hacer estas indicaciones. Primeramente, actualice su información directamente con el banco. Segundo, verifique sus transacciones diariamente. Tercero, si recibe información o una llamada de teléfono que quiera actualizar nuevos pagos o nuevos conductores para su cuenta, verifique directamente con su agente bancario para saber que esas transacciones sean reales.

GRÁFICO EN PANTALLA: ¿Qué debo hacer si identifico un correo electrónico, un mensaje de texto u otra comunicación fraudulenta?

>> Núñez: Si usted recibe un correo electrónico, o un mensaje de texto que pueda provenir de un estafador, si lo ve, si lo detecta, repórtelo, y lo puede reportar mandándonos un email aquí a Wells Fargo a: el correo electrónico reportphish que es reportphish@wellsfargo.com. También puede mandarle la información a: el www.ftc.gov/

GRÁFICO EN PANTALLA: © 2020 Wells Fargo Bank, N.A. Todos los derechos reservados.