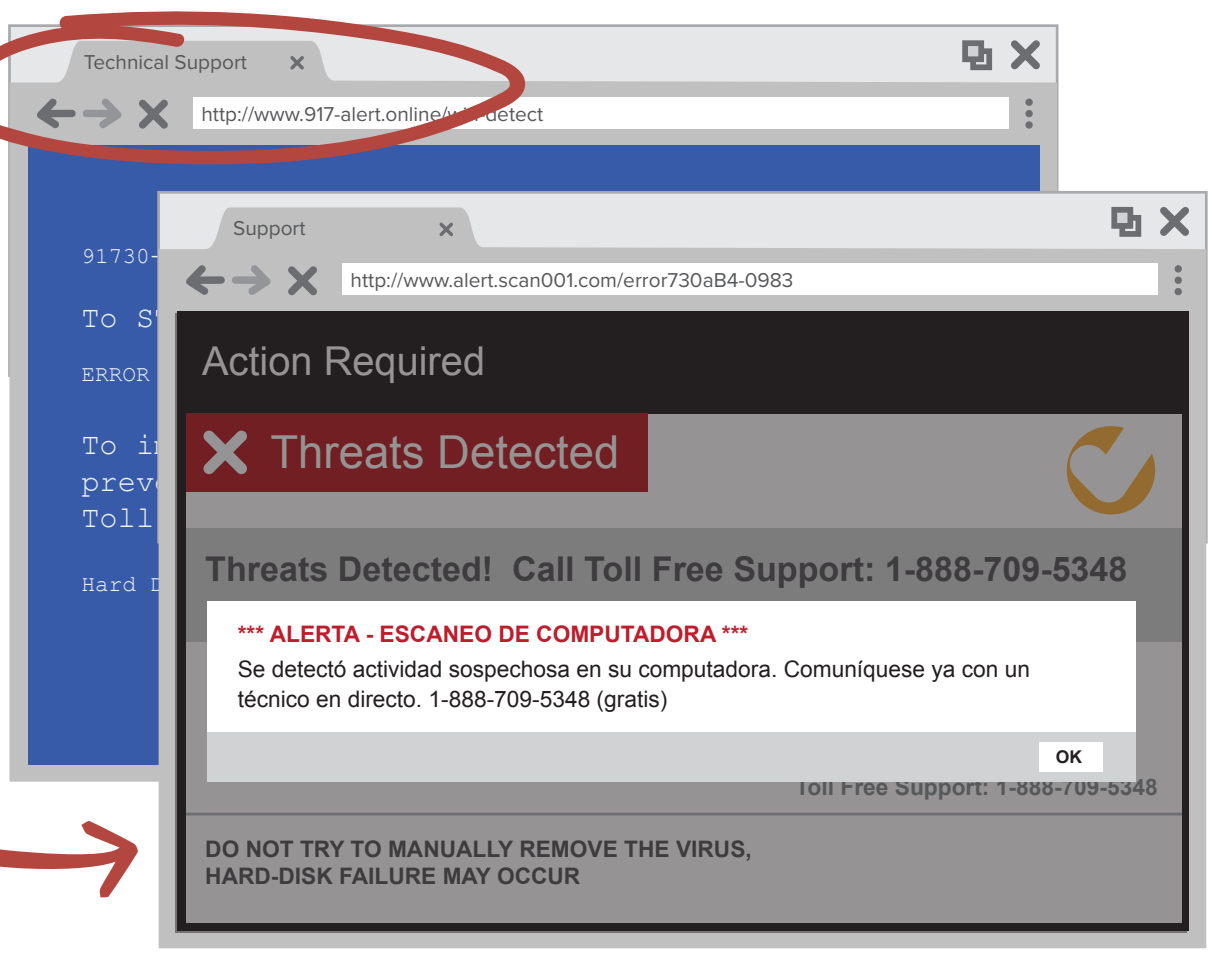
CÓMO DETECTAR UNA

ESTAFA DE SOPORTE TÉCNICO

A menudo comienza con un mensaje pop-up . . .

Aparece dentro de su **navegador de internet**



Podría **imitar** una pantalla azul de error

o un software antivirus confiable

LLAME	AHORA	O DE LO CONTRARIO...
Le indica que llame a un **número gratuito**	Lo urge a llamar **inmediatamente**	Lo amenaza con la **pérdida de sus datos personales** si no llama

Entonces, usted llama a un número gratuito. El estafador podría:

- Pedirle que le ceda acceso remoto.
- Pedirle que le ceda acceso remoto.
- Decirle que encontraron un virus u otro problema de seguridad.
- Tratar de venderle servicios de reparación o una suscripción de seguridad.

Luego le piden que pague un cargo.

El estafador provee "servicios" que van desde:

INSERVIBLES

- Cosas que usted puede conseguir gratis en otro lado.
- Cosas que ya tiene.
- "Reparar" un problema inexistente.
- Suscripciones que no sirven para nada.
- Instalar programas maliciosos

MALICIOSOS

LO QUE PUEDE HACER:

- Si recibe un mensaje tipo pop-up, un email spam o cualquier otro tipo de mensaje urgente acerca de un virus en tu computadora, **pise el freno**.

  No haga clic en ningún enlace ni llame a ningún número de teléfono.

  No envíe dinero.

  No le ceda a nadie el control sobre su computadora

  Microsoft no envía advertencias de tipo pop-up para pedirle que llame a un número gratuito acerca de virus o problemas de seguridad.

- **Repórtelo** en ftc.gov/queja. Incluya el número de teléfono al que le indicaron que llamara.

- Mantenga actualizado **su software de seguridad**. Sepa cómo luce para que pueda detectar una falsificación.

- **Informe** a los demás sobre esta estafa. Podría ayudarlos a detectar y evitar una llamada costosa.

APRENDA MÁS EN: ftc.gov/estafasdesoportetecnico