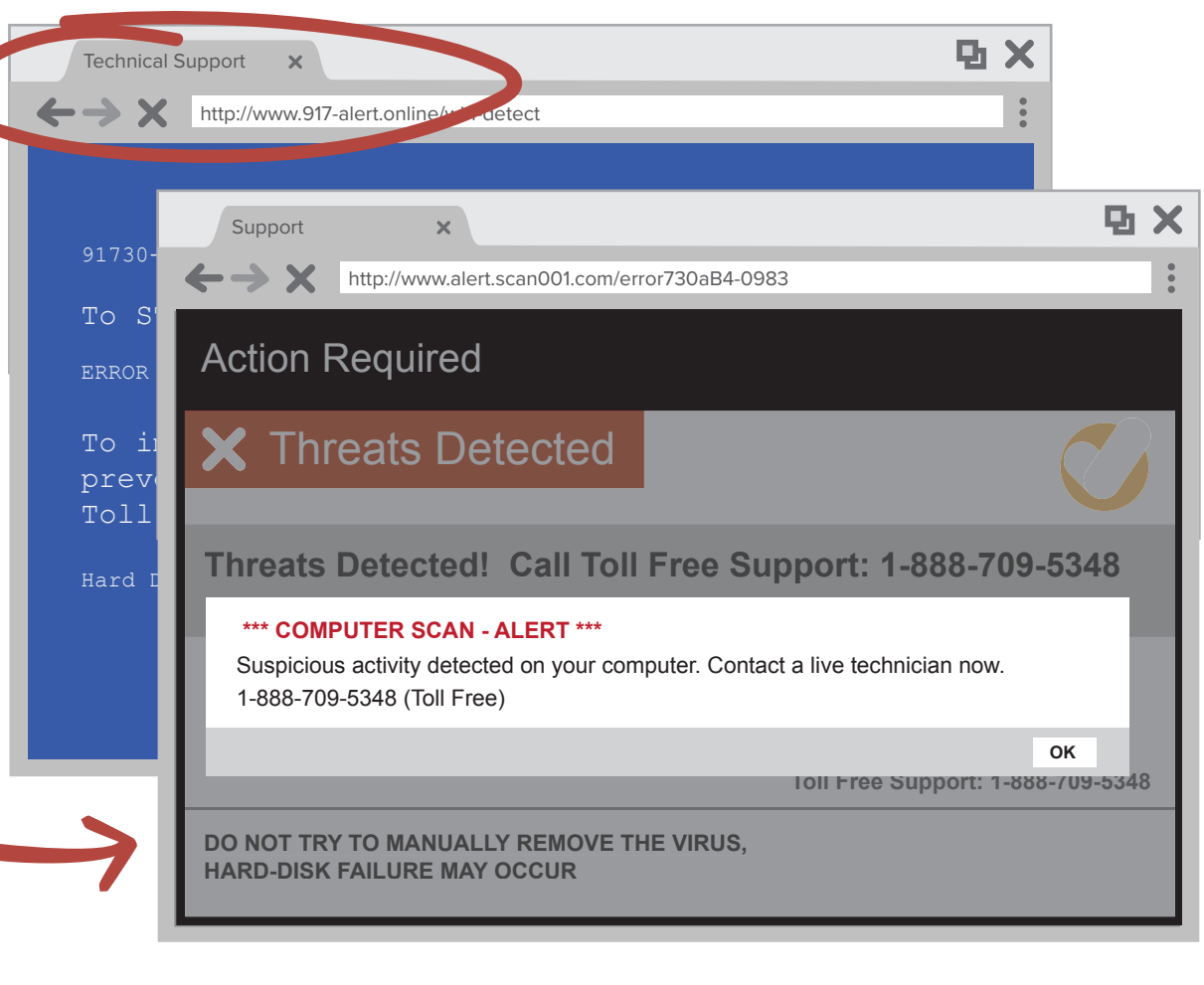
HOW TO SPOT A
TECH SUPPORT SCAM

It often starts with a pop-up . . .

Shows up within your **internet browser**



Might **imitate** a blue error screen

or trusted antivirus software

CALL	NOW	OR ELSE...
Wants you to call a **toll-free number**	Urges you to call **immediately**	Threatens that you may **lose personal data** if you don't call

Then, you call a toll-free number. The scammer might:

- ask you to give them remote access
- pretend to run a diagnostic test
- tell you they've found a virus or other security issue
- try to sell you repair sevices or a security subscription

Then, you're asked to pay a fee.

The scammer provides "services" that range from:

WORTHLESS

- things you can get elsewhere for free
- things you already have
- "fixing" a problem that doesn't exist
- subscriptions that don't do anything
- installing malware

MALICIOUS

WHAT YOU CAN DO:

- If you get a pop-up, call, spam email or any other urgent message about a virus on your computer, **stop**.

  Don't click on any links or call a phone number.

  Don't send any money.

  Don't give anyone control of your computer.

  Microsoft does not display pop-up warnings and ask you to call a toll-free number about viruses or security problems.

- **Report it** at ftc.gov/complaint. Include the phone number that you were told to call.

- Keep **your security software** up to date. Know what it looks like so you can spot a fake.

- **Tell someone** about this scam. You might help them spot it and avoid a costly call.

LEARN MORE: ftc.gov/TechSupportScams