

NAPLES COMPUTERS HOW-TO • BUSINESS I.T.

The First Hour After a Cyberattack (Small Business)

If you suspect your business just got hit by ransomware or another cyberattack, the first hour matters. This guide covers what to actually do, based on official CISA guidance: isolate, don't power off, don't pay on impulse, and who to call.

Three instincts to **fight**

The natural reaction is usually the wrong one.

Don't just power it off

Shutting a computer down can destroy evidence stored in its memory.

Don't pay out of panic

A free way to undo it may already exist; paying doesn't guarantee anything.

Don't delete anything

The ransom note and any strange files are evidence, not clutter.

Step by step

STEP 1**Disconnect it, but leave it running**

Unplug the network cable, or turn off Wi-Fi, on any affected computer. Leave the power on.

WHAT TO DO

This stops it from spreading to other computers, while keeping evidence intact for whoever investigates.



Cut off **the network**, not the power

STEP 2



Take a breath before you do anything else

Photograph or write down what you're seeing. Don't pay a ransom on impulse; a free decryption tool may already exist.

WHAT TO DO

CISA and the FBI both discourage paying; it doesn't guarantee you'll get your files back.



Document **first**, decide later

STEP 3

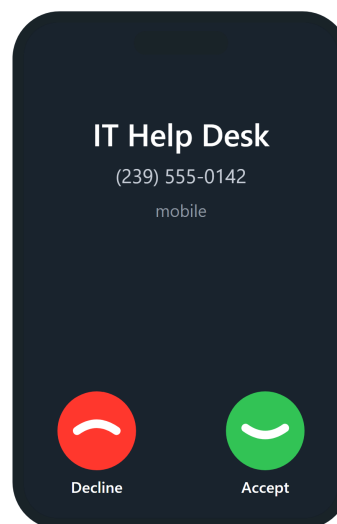


Call your IT provider, then report it

Use a phone call or text, not email; your email system might be compromised too.

WHAT TO DO

CISA, the FBI's Internet Crime Complaint Center (IC3), and your cyber insurance carrier (if you have one) should all hear from you.



Call, **don't email**, your IT provider

A few tips



Have a plan before it happens

Decide now who's in charge and who gets called, not during the panic



Don't try to fix it yourself

If you're not sure what you're doing, you can make it worse or destroy evidence

- ☐ Keep a written timeline
What you noticed, and when; it helps whoever investigates afterward

Recap: the first hour

- ☐ Isolate the computer; disconnect it, don't power it off
- ☐ Don't pay on impulse; document what you're seeing
- ☐ Call your IT provider by phone or text, not email
- ☐ Report it to CISA, the FBI, and your insurance carrier

The instinct to power off a compromised computer is usually wrong; it can destroy evidence stored in memory. Disconnect it from the network instead, and leave the power on.



Think your business has been compromised?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**