

The First Hour After an Attack

What to actually do, for a small business.



*We Make
I.T.
Happen!™*

1 Don't Just Power It Off

Shutting down can **destroy** evidence stored in memory.



2 Don't Pay Out of Panic

A free decryption tool **may already** exist.



3 Step 1: Isolate It

Unplug the network cable, or turn off Wi-Fi. **Leave the power on.**



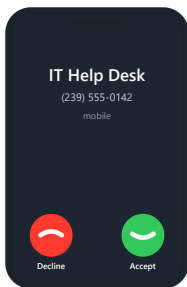
4 Step 2: Document Everything

Photograph or write down **what** you're seeing.



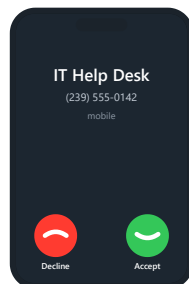
5 Step 3: Call Your IT Provider

Use a phone call or text, **not email.**



6 Report It

To CISA, the FBI's IC3, and your **cyber insurance carrier.**



7 Have a Plan Before It Happens

Decide now who's in charge, **not** during the panic.



8 Keep a Written Timeline

What you noticed, and when; it **helps the investigation.**



Good to Know

- Disconnect from the network, don't power off; shutting down can destroy evidence.
- CISA and the FBI both discourage paying a ransom on impulse.
- Think your business has been compromised? Call **239-513-1960** right away.



Need Help?

Contact Naples Computers

239-513-1960

We Make I.T. Happen!™