Ransomware Scare & Infected Computer

The Situation

An employee opens an unexpected email attachment and suddenly notices unusual behavior on their computer.

Files appear inaccessible. Pop-ups begin appearing. The employee is worried that the business may have been hit by ransomware.

They immediately shut down the computer and contact IT.

The Challenge

The business needs to determine:

- Is the computer actually infected?
- Has ransomware executed?
- Has malware spread to other systems?
- Are company files at risk?
- Can the computer safely reconnect to the network?
- Are backups available if files have been encrypted?

The Reconnect IT Approach

The first priority is **containment**.

Reconnect IT can work with the business to isolate the affected device and assess the situation before reconnecting it to the network.

We can:

1. Contain the threat
Isolate the potentially compromised device to reduce the possibility of further spread.

2. Assess the situation
Determine what occurred and whether there are indicators of malware or ransomware activity.

3. Check surrounding systems
Review other potentially affected devices and accounts where appropriate.

4. Assess backups
Determine whether critical business data is protected and whether usable recovery points are available.

5. Remediate the affected system
Remove the threat or recommend rebuilding the affected device when that is the safer option.

6. Strengthen security
Provide recommendations for endpoint protection, Microsoft 365 security, backups, user awareness and other controls.

The Result

The objective isn't simply to get one computer working again.

It's to determine whether the business is safe to continue operating and reduce the possibility of the incident becoming something much larger.

Key Takeaways

- Potentially compromised device isolated
- Threat assessed
- Other systems considered
- Backup availability reviewed
- Device remediated or rebuilt as appropriate
- Security recommendations provided

The Bottom Line

When ransomware is suspected, **every minute matters.**

Don't reconnect a potentially infected computer and hope for the best.

Disconnect. Contain. Call Reconnect IT.