



Troubleshooting Methodology

THOMAS HOLT RUSSELL, M.ED, HON. D. (CYBERSECURITY)

What is Troubleshooting?

- Troubleshooting is a **systematic approach** to diagnosing and resolving IT issues.
- The **CompTIA IT Fundamentals (ITF+)** exam outlines a **structured methodology** for effective problem resolution.
- This methodology applies to **hardware, software, networking, and cybersecurity** issues.

```
mirror_mod = modifier_ob.  
#set mirror object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
#selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly  
-- OPERATOR CLASSES --  
  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
  
context):  
context.active_object is not
```

The 8-Step Troubleshooting Process



Identify the problem



Research knowledge base/internet



Establish a theory of probable cause



Test the theory to determine the cause



Establish a plan of action and identify potential effects



Implement the solution or escalate



Verify full system functionality and apply preventive measures



Document findings, actions, and outcomes

Step 1 - Identify the Problem

- Gather information from the user.
- Replicate the issue if possible.
- Check logs, error messages, and recent changes.

Example:

A user reports that their computer won't turn on. You check power connections and listen for beep codes.

Step 2 - Research Knowledge Base/Internet

Use **vendor documentation, online forums, and error code lookups.**

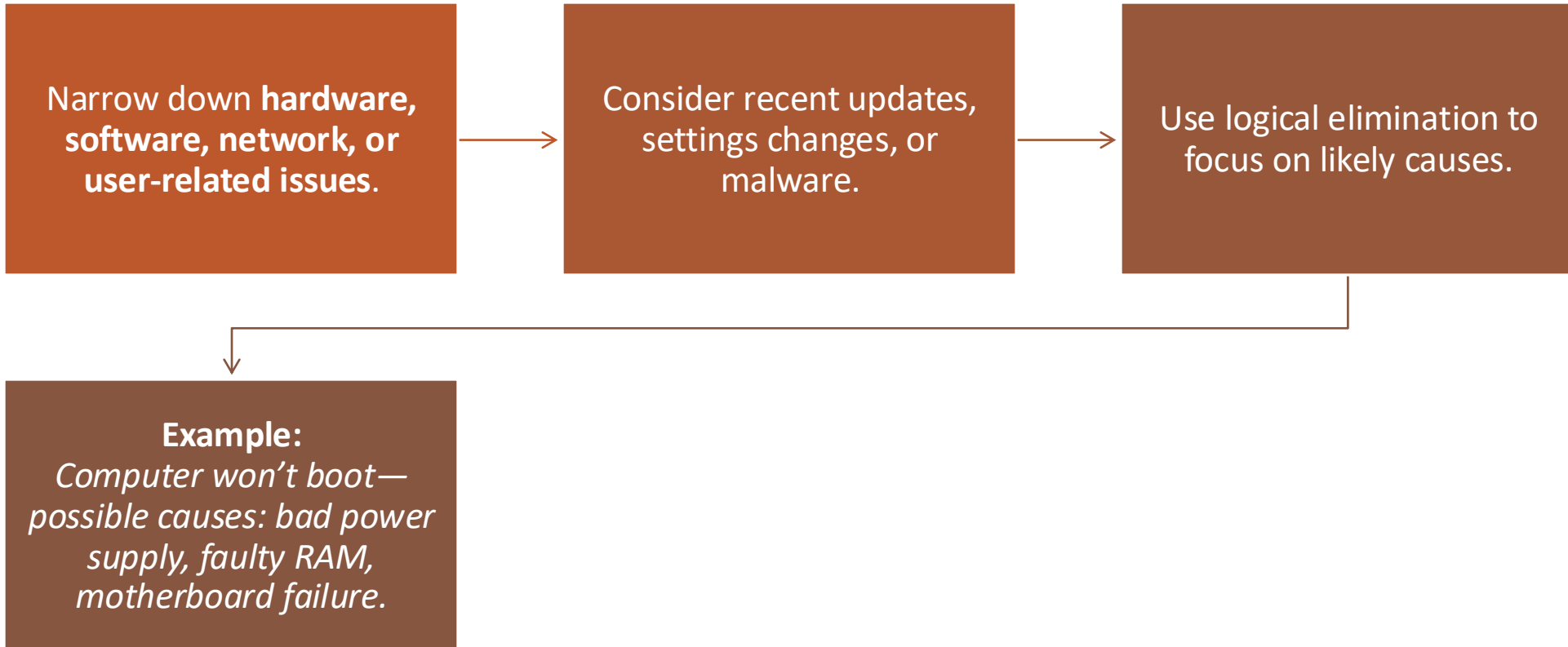
Check company IT records for similar cases.

Search IT forums like **Stack Overflow, Reddit, and manufacturer support sites.**

Example:

A Windows update caused an issue—check Microsoft forums for known problems.

Step 3 - Establish a Theory of Probable Cause



Step 4 - Test the Theory to Determine the Cause

- Try **quick tests** (restart, swap cables, check task manager).
- Run **diagnostic tools** (ping, ipconfig, hardware tests).
- If the issue persists, **reassess your theory**.

Example:

Wi-Fi is slow → Run a speed test → Background software update is consuming bandwidth.

Choose the **least disruptive solution** first.



Consider **potential side effects** of your fix.



Step 5 - Establish a Plan of Action

Example:

Fixing a corrupted system file? Back up important data before restoring it.



Backup data before making major changes.

Apply the fix and
monitor the results.

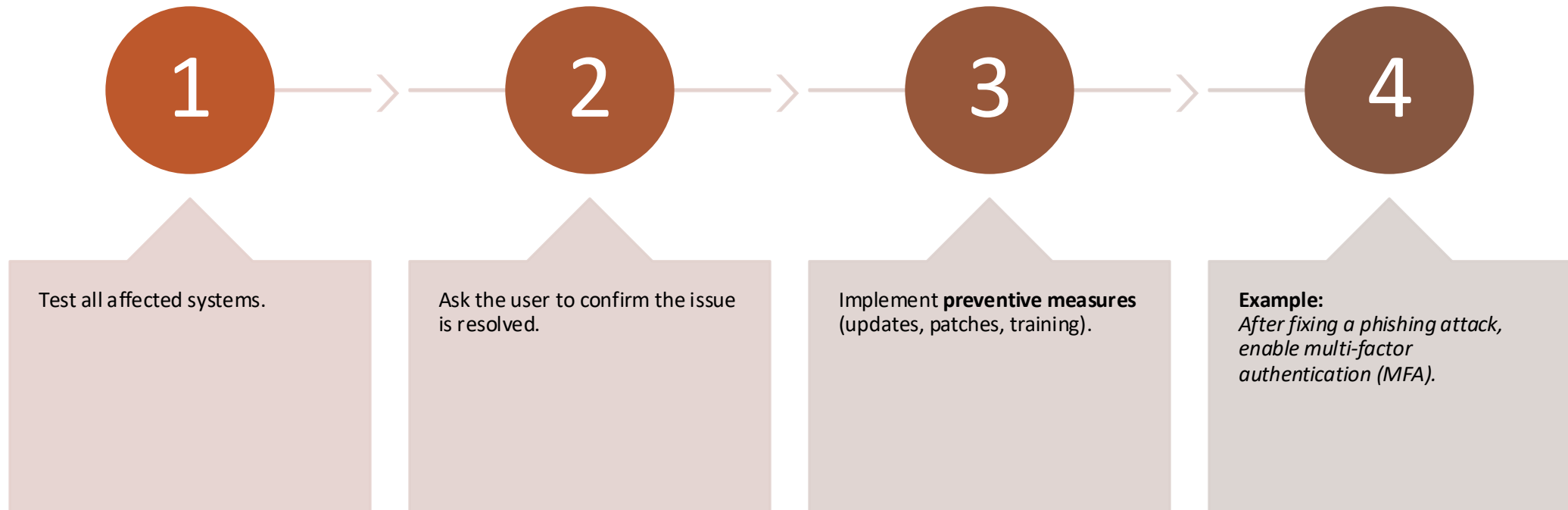
If unsuccessful, escalate
to a senior technician or
vendor support.

Document the solution
steps for reference.

Example:
*Firewall blocks VPN
traffic—modify firewall
settings, then test
connectivity.*

Step 6 - Implement the Solution or Escalate

Step 7 - Verify Full System Functionality



Step 8 - Document Findings & Lessons Learned

- Record the **problem, troubleshooting steps, and resolution.**
- Update company knowledge base.
- Improve training or security policies if needed.

Example:

Documenting a known bug in accounting software for future reference.



Case Study - Cybersecurity Incident

**Phishing Attack
Compromised Email
Account**

The employee clicked
a fake IT support
email and entered
credentials.

IT checked login
logs—unauthorized
access detected.

Solution: Forced
password reset,
enabled MFA, and
educated employees.

Preventive Measure:
Improved **email
filtering and phishing
simulations.**

Case Study - Healthcare IT Downtime

**Hospital EHR System
Failure**

Doctors couldn't
access patient
records.

IT checked server
logs—high CPU usage
due to a faulty
update.

Solution: Rolled back
update, restarted
servers.

Preventive Measure:
Scheduled **test
environments before
future updates.**

Case Study - VPN Failure in Enterprise

Remote Employees Unable to Connect to VPN

Multiple employees reported VPN login failures.

IT found that a firewall update was blocking VPN traffic.

Solution: Adjusted firewall settings, restarted VPN servers.

Preventive Measure: **Automated alerts for VPN downtime.**

Key Takeaways

Follow	Follow structured troubleshooting steps to resolve IT issues efficiently.
Test	Always test solutions and verify full functionality.
Implement	Implement preventive measures to reduce future issues.
Document	Document findings to improve IT processes.

Q&A

QUESTIONS?





Troubleshooting Methodology

THOMAS HOLT RUSSELL, M.ED, HON. D. (CYBERSECURITY)