



**IT CAREER KIT
MYSOFTWAREUSB**

IT Career Starter Pack

A practical, no-cost toolkit for IT support, networking, software, and technology careers.

Inside: resume prompts • interview practice • troubleshooting checklist • Windows commands • security habits • 30-day learning plan

Prepared as a free digital welcome gift for MySoftwareUSB members.

Welcome — make this pack useful

This pack is designed to help you prepare for IT roles, explain your skills clearly, and work through common support issues in a more structured way. Use the templates as a starting point and adapt them to your real experience.

Your 20-minute setup checklist

- Pick one target role. Examples: IT Support Technician, Help Desk Analyst, Network Technician, Junior Developer, QA Tester, or Cloud Support Associate.
- Write down six real skills. Include tools, systems, platforms, and tasks you can confidently explain in an interview.
- Collect proof of practice. Save a small project, lab notes, screenshots, or a troubleshooting write-up. Do not include employer or customer confidential data.
- Update your resume. Keep it readable, accurate, and tailored to the role.
- Practice out loud. Explain one technical issue in simple language, then describe how you would test and resolve it.

Important: this pack is educational. A MySoftwareUSB member badge or resource access is not a guarantee of employment, certification, or independently verified job history.

A simple career goal

In the next 30 days, I will practise _____ for _____ minutes per week and complete _____ as evidence of my learning.

Resume builder: clear, honest, relevant

Use this outline to build a one- or two-page resume. Keep claims truthful and be ready to explain each skill or achievement.

Suggested structure

SECTION	WHAT TO INCLUDE
Contact	Name • professional email • phone • city • LinkedIn/portfolio (optional). Do not put government ID numbers or full home address on a public resume.
Summary	2–3 lines: target role, strongest relevant skills, and the type of problems you can help solve.
Skills	Group skills such as Windows/Linux, networking, ticketing systems, scripting, databases, testing, or cloud tools. List only what you can discuss.
Experience	For each role: title, employer, dates, and 3–5 concise bullets describing your own work.
Projects	Project name • goal • tools used • what you built/tested • what you learned. Personal labs are valid if clearly labelled as projects.
Learning	Relevant courses, labs, certifications, and dates. Do not describe a course as a professional certification unless it actually is one.

Achievement bullet formula

Action + tool/context + result. Example structure: “Resolved [type of issue] using [tool/process], reducing [impact] by [measured result].” Only add a number or result if you can verify it.

Project notes template

Project: _____
Problem or goal: _____
Tools used: _____
My contribution: _____
What I learned: _____

Interview practice: 8 useful prompts

Use the prompts below to practise short, structured answers. For technical questions, explain what you would check first, how you would test, and how you would confirm the fix.

1. Tell me about yourself.

Give a 30–60 second summary of your target role, relevant experience or projects, core skills, and next goal.

2. A user cannot connect to the internet. What do you do?

Check scope, Wi-Fi/cable, IP settings, gateway, DNS, a known-good site, and whether other users/devices are affected. Record results and escalate with evidence.

3. What is DNS?

DNS translates domain names into IP addresses. If name lookups fail but connectivity works, test name resolution and compare with a known working host.

4. What is DHCP?

DHCP automatically provides network configuration such as IP address, subnet mask, gateway, and DNS servers.

5. How do you prioritise support tickets?

Consider business impact, number of users affected, urgency, security implications, and the organisation's agreed SLA. Communicate the expected next step.

6. How do you handle an unfamiliar issue?

Clarify symptoms, gather exact errors, check documentation, make one controlled change at a time, and ask for help/escalate when appropriate.

7. What is MFA and why use it?

Multi-factor authentication adds another proof of identity beyond a password and can reduce risk if a password is stolen.

8. Describe a project or problem you solved.

Use STAR: Situation, Task, Action, Result. Be clear about your personal contribution and what you learned.

Interview tip: it is better to say “I have not used that tool yet, but here is how I would learn and test it” than to claim experience you do not have.

IT troubleshooting: repeatable workflow

A consistent process prevents guesswork and makes handoffs clearer. Follow your organisation's policies and change-control rules.

1. Define the issue

Ask what changed, when it started, the exact error, and who/what is affected.

2. Set the scope

One user or many? One device or all devices? One application or the whole system?

3. Check the basics

Power, cables, connectivity, account status, available storage, recent updates, and service status.

4. Gather evidence

Capture error text, time, relevant logs, device/OS details, and steps already tried. Avoid collecting unnecessary personal data.

5. Test one thing at a time

Use the least disruptive test first. Note what changed and the outcome.

6. Apply an approved fix

Follow documentation and change policies. Back up data or get approval before risky changes.

7. Confirm and document

Confirm with the user, document the cause and resolution, and note any follow-up needed.

8. Escalate responsibly

If unresolved or outside your access/skill, pass on concise evidence and actions already attempted.

Do not bypass access controls, disable security software, or run destructive commands just to make an alert disappear. Follow authorised support procedures.

Windows quick-reference commands

Run commands only on devices you are authorised to troubleshoot. Some commands show sensitive system details; avoid sharing full output publicly.

COMMAND	PURPOSE / CAUTION
ipconfig	Show basic IP configuration.
ipconfig /all	Show detailed adapter, DHCP, gateway, and DNS information.
ping	Test reachability/latency to a host; a failed ping does not always mean a host is down.
nslookup	Check DNS name resolution.
tracert	Show the path attempts to take toward a host.
whoami	Show the current signed-in account.
systeminfo	Show operating system and system details; review before sharing.
sfc /scannow	Check protected Windows system files; may require an elevated terminal and can take time.

Quick network triage

- Check the device link/Wi-Fi and whether others are affected.
- Use ipconfig to see whether an address and gateway are present.
- Use ping and nslookup as clues, not definitive proof.
- Record results and follow the approved escalation path.

Never paste credentials, tokens, private IP maps, or complete system diagnostics into public forums.

Security habits for every IT professional

Small, consistent habits protect users, employers, and your own accounts.

Account protection

Use unique passwords and MFA where available. Never share passwords, one-time codes, recovery codes, or sessions.

Phishing awareness

Check the sender, domain, unexpected urgency, attachments, and links. Verify unusual requests using a separate trusted channel.

Least privilege

Use only the access needed for your task. Do not borrow another person's account or bypass approvals.

Patch and update

Apply approved updates promptly; follow change windows and test requirements for managed systems.

Data handling

Share only necessary information. Remove customer names, credentials, and confidential data from examples and screenshots.

Backups and recovery

Understand what is backed up, how restore is tested, and who can approve a recovery action.

Safe remote support

Verify the user and the support request. Use organisation-approved remote access tools only.

Responsible disclosure

Report suspected incidents quickly through the designated process. Preserve evidence and avoid unauthorised investigation.

If you think an account or device is compromised, notify the authorised security/support team promptly. Do not delete evidence or attempt unauthorised access.

A practical 30-day growth plan

Keep the plan small enough to finish. Aim for regular practice rather than collecting courses without applying what you learn.

WEEK	FOCUS	DELIVERABLE
1	Choose a target role and map its common skills.	A one-page skills gap list.
2	Learn/practise one core topic: networking, Windows, coding, databases, QA, or cloud fundamentals.	Notes plus 5 practice questions.
3	Complete a small lab or personal project.	A short write-up or demo that contains no confidential data.
4	Update your resume and practise explaining your project.	One tailored resume and one mock interview.

Free learning resources

[Microsoft Learn](#) — Product documentation and guided learning paths.

[Cisco Skills for All](#) — Networking and cybersecurity learning content.

[freeCodeCamp](#) — Hands-on programming and web development practice.

[GitHub Skills](#) — Guided practice with GitHub workflows.

[AWS Skill Builder](#) — Cloud learning content; free and paid offerings may both be available.

Free access and course availability can change. Check each provider's current terms before starting a course or claiming a credential.

My application tracker

ROLE / COMPANY	DATE APPLIED	NEXT ACTION	STATUS
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Wishing you steady progress in your IT career.

MySoftwareUSB • Free member resource • mysoftwareusb.com