Cyber Defense Basics

Ages 13-15 | Tech Builders

Learn safe defense ideas using a paper or simulated home network.

How to use this guide

Read each section, complete its four lab steps, then answer the questions in the online course. The online progress bar advances only after four correct answers.

Section 1: Threats

LEARNING GOAL: Threats. Your finished work should demonstrate: A simple threat map.

EXPLAIN THE CONCEPT: A threat is something that may harm a device or account. Defense starts by noticing what needs protection. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.

ORIGINAL PROJECT LAB: 1. Draw a pretend home network with two devices. 2. Mark the information each device holds. 3. List two possible problems such as lost access or a suspicious message. 4. Choose which problem you will address first. Finished result: A simple threat map.

EXPLAIN THE MECHANISM: An asset is something worth protecting. A threat could harm it; a weakness can make that harm easier. A control reduces a particular risk but does not guarantee that nothing can go wrong. Identify what you are protecting before choosing a defense.

WORKED CASE: In a fictional club, an account stores project drafts. Reusing its password elsewhere is a weakness. Someone trying a leaked password is a threat. A unique password and an additional sign-in factor reduce that account-access risk, but do not repair every device problem.

TEST AND JUSTIFY: Make a paper table of asset, possible harm, weakness, and matching control. Use imaginary accounts only. Explain why a control fits the harm rather than listing tools at random. Do not investigate real accounts, devices, or networks without permission.

GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.

SAFETY CHECK: Recognize phishing and social engineering, secure accounts, understand privacy settings, and perform cyber labs only with authorization. Use pretend data,

never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A simple threat map.

Investigate with pictures and choices

A fictional email asks for a password urgently.

Which feature is a warning sign?

1. The greeting alone proves safety
2. The logo guarantees identity
3. The unexpected secret request

Worked reasoning

Answer: The unexpected secret request. Inspect the request and verify through a trusted route.

Try a changed example

Compare two messages with the same logo and different requests.

Picture and meaning matches

Threat: Could cause harm

Network boundary: Connects permitted systems

Access control: Limits an action

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool. A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed. Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Draw a pretend home network with two devices.
2. Mark the information each device holds.
3. List two possible problems such as lost access or a suspicious message.
4. Choose which problem you will address first.

Finished result: A simple threat map.

Check your understanding

1. Which idea best describes Threats?

A. It has no purpose in this project.

B. Devices use a network to communicate.

C. A threat is something that may harm a device or account.

D. Updates, unique passwords, and careful account settings reduce common risks.

2. What is the first step in this lab?

A. Choose which problem you will address first.

B. Mark the information each device holds.

C. List two possible problems such as lost access or a suspicious message.

D. Draw a pretend home network with two devices.

3. What should you do after step two?

A. List two possible problems such as lost access or a suspicious message.

B. Mark the information each device holds.

C. Choose which problem you will address first.

D. Draw a pretend home network with two devices.

4. Which result shows that your lab is finished?

A. A blank page with no work

B. A simple threat map.

C. A copied answer without checking it

D. A skipped lab

Answer review

1. C. A threat is something that may harm a device or account.
2. D. Start with: Draw a pretend home network with two devices.
3. A. Step three is: List two possible problems such as lost access or a suspicious message.
4. B. The goal is: A simple threat map.

Section 2: Networks

LEARNING GOAL: Networks. Your finished work should demonstrate: A labeled network

map.

EXPLAIN THE CONCEPT: Devices use a network to communicate. A router connects local devices and often provides settings for safer access. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.

ORIGINAL PROJECT LAB: 1. Label the router and devices on your drawing. 2. Draw which devices connect through it. 3. Mark a guest connection separately if your plan has one. 4. Explain to a partner where information enters the network. Finished result: A labeled network map.

EXPLAIN THE MECHANISM: A network lets devices exchange information. A router can connect networks; a home router often also provides Wi-Fi and other functions. Knowing a device’s network address is not the same as having permission to access it. Practice with diagrams instead of scanning.

WORKED CASE: Draw a fictional laptop, router, and web service. Trace a request from the laptop through the router to the service and the response back. Label the points where identity or access might be checked. A connected device is not automatically trusted.

TEST AND JUSTIFY: Add a pretend guest device and explain why you might separate its access from private devices. State what the diagram leaves out. Ask an adult before changing any router setting; the reading activity does not require a real network change.

GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.

SAFETY CHECK: Recognize phishing and social engineering, secure accounts, understand privacy settings, and perform cyber labs only with authorization. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A labeled network map.

Investigate with pictures and choices

A classroom network diagram has a public service and private database.

What should the boundary do?

1. Treat every source as trusted
2. Allow only required connections
3. Expose every port

Worked reasoning

Answer: Allow only required connections. Network access should match the required communication paths.

Try a changed example

Draw the permitted direction of a request and response.

Picture and meaning matches

Threat: Could cause harm

Network boundary: Connects permitted systems

Access control: Limits an action

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Label the router and devices on your drawing.
2. Draw which devices connect through it.
3. Mark a guest connection separately if your plan has one.
4. Explain to a partner where information enters the network.

Finished result: A labeled network map.

Check your understanding

1. Which idea best describes Networks?

A. A threat is something that may harm a device or account.

B. Devices use a network to communicate.

C. Updates, unique passwords, and careful account settings reduce common risks.

D. It has no purpose in this project.

2. What is the first step in this lab?

A. Draw which devices connect through it.

B. Mark a guest connection separately if your plan has one.

C. Label the router and devices on your drawing.

D. Explain to a partner where information enters the network.

3. What should you do after step two?

A. Draw which devices connect through it.

B. Explain to a partner where information enters the network.

C. Label the router and devices on your drawing.

D. Mark a guest connection separately if your plan has one.

4. Which result shows that your lab is finished?

A. A labeled network map.

B. A copied answer without checking it

C. A skipped lab

D. A blank page with no work

Answer review

1. B. Devices use a network to communicate.

2. C. Start with: Label the router and devices on your drawing.

3. D. Step three is: Mark a guest connection separately if your plan has one.

4. A. The goal is: A labeled network map.

Section 3: Defense

LEARNING GOAL: Defense. Your finished work should demonstrate: A defense plan with reasons.

EXPLAIN THE CONCEPT: Updates, unique passwords, and careful account settings reduce common risks. Make changes only on a simulated plan or with permission. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.

ORIGINAL PROJECT LAB: 1. Choose three safe settings for your pretend network. 2. Place each setting on the network map. 3. Explain which problem each setting reduces. 4. Review your plan with a trusted adult before changing any real device.

Finished result: A defense plan with reasons.

EXPLAIN THE MECHANISM: Useful defenses address different failure modes. Updates repair known software problems; unique secrets reduce reuse risk; access limits reduce unnecessary permissions; backups can support recovery. One control does not replace the others. Apply changes only with authorization.
WORKED CASE: A fictional tablet is missing updates and has no backup of a project. An update helps software security but does not restore a deleted drawing. A separate backup can help recover the drawing if it contains a usable saved copy.
TEST AND JUSTIFY: Build a simulated improvement plan: identify the risk, propose a control, and describe how an authorized adult would check it worked. Never disable protections to make a demonstration easier. Label untested proposals as plans, not verified results.
GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.
SAFETY CHECK: Recognize phishing and social engineering, secure accounts, understand privacy settings, and perform cyber labs only with authorization. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.
REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.
PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A defense plan with reasons.

Investigate with pictures and choices

A viewer account can delete records.
What control should be reviewed?
1. Permissions for the viewer role
2. Only the page font
3. Whether all accounts share credentials

Worked reasoning

Answer: Permissions for the viewer role. Access rights should match the task and authorized role.

Try a changed example

Test both an allowed read and a forbidden deletion in a mock.

Picture and meaning matches

Threat: Could cause harm

Network boundary: Connects permitted systems

Access control: Limits an action

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Choose three safe settings for your pretend network.
2. Place each setting on the network map.
3. Explain which problem each setting reduces.
4. Review your plan with a trusted adult before changing any real device.

Finished result: A defense plan with reasons.

Check your understanding

1. Which idea best describes Defense?

A. It has no purpose in this project.

B. A threat is something that may harm a device or account.

C. Updates, unique passwords, and careful account settings reduce common risks.

D. Devices use a network to communicate.

2. What is the first step in this lab?

A. Review your plan with a trusted adult before changing any real device.

B. Place each setting on the network map.

C. Explain which problem each setting reduces.

D. Choose three safe settings for your pretend network.

3. What should you do after step two?

A. Explain which problem each setting reduces.

B. Place each setting on the network map.

C. Review your plan with a trusted adult before changing any real device.

D. Choose three safe settings for your pretend network.

4. Which result shows that your lab is finished?

A. A blank page with no work

B. A defense plan with reasons.

C. A copied answer without checking it

D. A skipped lab

Answer review

1. C. Updates, unique passwords, and careful account settings reduce common risks.

2. D. Start with: Choose three safe settings for your pretend network.

3. A. Step three is: Explain which problem each setting reduces.

4. B. The goal is: A defense plan with reasons.

Section 4: Guided Project & Worked Examples

COURSE INVESTIGATION: A scan result needs a scope

YOUR PRACTICE INPUT: A fictional inventory lists two laptops and one printer. A practice scan covers only the laptops and reports no known critical findings.

WHY IT WORKS: A result applies to the checked assets, configuration, time, and detection rules. It does not prove that an unscanned printer is secure.

PLAN BEFORE YOU ACT: Draw or write the starting state, the question you need to answer, and the evidence you expect to see. A paper trace is acceptable; label it as a prediction unless you actually run a test.

WORK THE CASE: Prepare a coverage table with checked, unchecked, and unknown states. Prioritize a safe follow-up plan on paper.

COMPARE WITH THE EXPECTED RESULT: The report identifies one checked asset and two coverage gaps. It never labels missing evidence as a clean result.

EXPLAIN YOUR REASONING: Show the connection between the supplied input, each decision, and your result. If a number, label, or observation differs, return to the first differing step rather than changing several things together.

KEEP YOUR EVIDENCE: Save the initial plan, a drawing or sanitized output, and one explanation of what the result does and does not prove. Use pointing, speech, drawing, typing, or your usual communication method.

LEARNING GOAL: Guided Project & Worked Examples. Your finished work should

demonstrate: A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.
EXPLAIN THE CONCEPT: Review the course concepts through two applied examples. Map assets, threats, vulnerabilities, and controls for a simulated home/school network. Analyze a pretend phishing email for sender mismatch, urgency, link destination, attachment risk, and credential request. Guided project: Create a simulated defense plan with network diagram, asset inventory, identity controls, patching, backups, logging, and incident steps. Work with synthetic or fictional information and ask an adult for help when appropriate. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.
ORIGINAL PROJECT LAB: 1. Read both worked examples and explain the reasoning. 2. Create a simulated defense plan with network diagram, asset inventory, identity controls, patching, backups, logging, and incident steps. 3. Record the steps you completed and the result you observed. 4. Compare your result to the goal and correct one issue. Finished result: A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.
EXPLAIN THE MECHANISM: Prepare a fictional club defense plan for accounts, devices, and project files. Keep the scope written down. You are analyzing a paper scenario, not trying to enter or test any real system. Separate observations from guesses.
WORKED CASE: The scenario states that passwords are reused, updates are delayed, and no backup is kept. Match unique passwords and extra sign-in protection to account risk, updates to known software weaknesses, and backups to recovery. Explain what each measure does not solve.
TEST AND JUSTIFY: Prioritize the proposed actions and name the evidence an authorized adult would need to verify them. Include one recovery check, such as opening a test backup copy. Do not claim a system is secure because a checklist contains ticks.
GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.
SAFETY CHECK: Recognize phishing and social engineering, secure accounts, understand privacy settings, and perform cyber labs only with authorization. Use pretend data,

never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Investigate with pictures and choices

A defense control blocks one test request.

What else must be checked?

1. Whether the slide looks convincing
2. Nothing else is relevant
3. Legitimate traffic still works

Worked reasoning

Answer: Legitimate traffic still works. A useful control handles both intended access and forbidden access.

Try a changed example

Create positive and negative test cases using synthetic data.

Picture and meaning matches

Threat: Could cause harm

Network boundary: Connects permitted systems

Access control: Limits an action

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool. A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed. Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Read both worked examples and explain the reasoning.
2. Create a simulated defense plan with network diagram, asset inventory, identity controls, patching, backups, logging, and incident steps.
3. Record the steps you completed and the result you observed.
4. Compare your result to the goal and correct one issue.

Finished result: A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Check your understanding

1. Which idea best describes Guided Project & Worked Examples?

A. A threat is something that may harm a device or account.

B. Review the course concepts through two applied examples.

C. Devices use a network to communicate.

D. It has no purpose in this project.

2. What is the first step in this lab?

A. Create a simulated defense plan with network diagram, asset inventory, identity controls, patching, backups, logging, and incident steps.

B. Record the steps you completed and the result you observed.

C. Read both worked examples and explain the reasoning.

D. Compare your result to the goal and correct one issue.

3. What should you do after step two?

A. Create a simulated defense plan with network diagram, asset inventory, identity controls, patching, backups, logging, and incident steps.

B. Compare your result to the goal and correct one issue.

C. Read both worked examples and explain the reasoning.

D. Record the steps you completed and the result you observed.

4. Which result shows that your lab is finished?

A. A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

B. A copied answer without checking it

C. A skipped lab

D. A blank page with no work

Answer review

1. B. Review the course concepts through two applied examples.
2. C. Start with: Read both worked examples and explain the reasoning.
3. D. Step three is: Record the steps you completed and the result you observed.
4. A. The goal is: A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Section 5: Independent Challenge & Mastery

INDEPENDENT TRANSFER CASE: A scan result needs a scope

KEEP THE ORIGINAL BASELINE: A fictional inventory lists two laptops and one printer. A practice scan covers only the laptops and reports no known critical findings.

CHANGE ONE CONDITION: One laptop was offline during the scan, leaving only one observed laptop.

YOUR TASK: Prepare a coverage table with checked, unchecked, and unknown states. Prioritize a safe follow-up plan on paper.

PREDICT, THEN CHECK: State which part of your original reasoning should remain true and which part must be recalculated or retested. Keep the original and changed results side by side.

REVIEW CRITERIA: The report identifies one checked asset and two coverage gaps. It never labels missing evidence as a clean result.

MENTOR DISCUSSION: Explain why the changed condition matters. Identify a tempting wrong conclusion, show the observation that would challenge it, and choose one next test. A statement of uncertainty is better than inventing a result.

PORTFOLIO NOTE: Keep your baseline, changed input, prediction, observed or paper-traced result, explanation, and one improvement. These practice prompts do not replace the course’s existing quiz or final assessment.

LEARNING GOAL: Independent Challenge & Mastery. Your finished work should demonstrate: An independent demonstration with evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

EXPLAIN THE CONCEPT: Apply what you learned without copying the guided solution. Independent challenge: Given a safe mock incident, identify indicators, contain on paper/simulation, preserve evidence, and write a short incident report. Safety and responsibility: Practice only on owned/authorized simulations. Never scan, access, disrupt, or test someone else’s account, device, network, or service. Reflect on your work: What did you build or discover? What did you test or change after

feedback? What safe or responsible choice did you make? Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.

ORIGINAL PROJECT LAB: 1. Explain the challenge and make a short plan. 2. Given a safe mock incident, identify indicators, contain on paper/simulation, preserve evidence, and write a short incident report. 3. Test the result and record evidence of your work. 4. Review the safety scenario and describe one improvement. Finished result: An independent demonstration with evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

EXPLAIN THE MECHANISM: Review a second fictional environment and propose three improvements. Choose different assets or constraints from the guided example. State what is given, what remains unknown, and which actions require an adult or authorized administrator.

WORKED CASE: A practice case reports an unfamiliar sign-in notice. That notice is an observation, not proof of who accessed the account. A safe recommendation is to involve an adult and review the service through an independent official route rather than the notice’s link.

TEST AND JUSTIFY: Produce a short defense brief with risks, proposed controls, verification steps, and limitations. Explain why you did not scan a real network or collect private account details. Responsible scope is part of the technical result.

GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.

SAFETY CHECK: Recognize phishing and social engineering, secure accounts, understand privacy settings, and perform cyber labs only with authorization. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: An independent demonstration with evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Investigate with pictures and choices

Someone suggests scanning a real neighbor network.

What should you do?

1. Hide the activity
2. Use only an authorized lab scope
3. Scan if it seems harmless

Worked reasoning

Answer: Use only an authorized lab scope. Cyber practice requires authorization and a defined scope.

Try a changed example

Write the allowed targets and stop conditions for a simulated lab.

Picture and meaning matches

Threat: Could cause harm

Network boundary: Connects permitted systems

Access control: Limits an action

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Explain the challenge and make a short plan.
2. Given a safe mock incident, identify indicators, contain on paper/simulation, preserve evidence, and write a short incident report.
3. Test the result and record evidence of your work.
4. Review the safety scenario and describe one improvement.

Finished result: An independent demonstration with evidence: Network/security

diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Check your understanding

1. Which idea best describes Independent Challenge & Mastery?

A. It has no purpose in this project.

B. A threat is something that may harm a device or account.

C. Apply what you learned without copying the guided solution.

D. Devices use a network to communicate.

2. What is the first step in this lab?

A. Review the safety scenario and describe one improvement.

B. Given a safe mock incident, identify indicators, contain on paper/simulation, preserve evidence, and write a short incident report.

C. Test the result and record evidence of your work.

D. Explain the challenge and make a short plan.

3. What should you do after step two?

A. Test the result and record evidence of your work.

B. Given a safe mock incident, identify indicators, contain on paper/simulation, preserve evidence, and write a short incident report.

C. Review the safety scenario and describe one improvement.

D. Explain the challenge and make a short plan.

4. Which result shows that your lab is finished?

A. A blank page with no work

B. An independent demonstration with evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

C. A copied answer without checking it

D. A skipped lab

Answer review

1. C. Apply what you learned without copying the guided solution.

2. D. Start with: Explain the challenge and make a short plan.

3. A. Step three is: Test the result and record evidence of your work.

4. B. The goal is: An independent demonstration with evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Mastery & safe-use plan

Ages 13-15

Digital safety: Recognize phishing and social engineering, secure accounts, understand privacy settings, and perform cyber labs only with authorization.

AI literacy: Evaluate bias, hallucinations, deepfakes, privacy risks, attribution,

and responsible model use.

Challenge: Complete an independent debugging, defense, data, or design scenario with documented reasoning.

Portfolio: Publish a sanitized project artifact with README-style purpose, steps, screenshots or evidence, and lessons learned.

Mastery check: Explain the design, demonstrate testing, identify a security or ethics risk, and defend one improvement.

Project worksheet

My project: Secure a simulated home network

Who will use or review it? _____

My plan: _____

Checkpoint 1: A simple threat map.

Checkpoint 2: A labeled network map.

Checkpoint 3: A defense plan with reasons.

Checkpoint 4: A completed guided project with documented evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

Checkpoint 5: An independent demonstration with evidence: Network/security diagram, Risk-control table, Incident worksheet, Lessons-learned report.

One thing I tested: _____

One thing I changed after testing: _____

What I learned: _____

Trusted adult or mentor feedback: _____

Family review

Show your finished work to a trusted adult. Explain one thing you learned and one thing you would improve.

Beat IT Kids | For learning at home. Do not put real passwords or private details in practice projects.