Hour of Code: Teacher Guide

CodeHS Cyber Range | Middle School Cyber Missions

Ten short cybersecurity missions that let students try the work real cyber professionals do: cracking passwords, spotting scams, defending a network, and solving a digital crime. No prior coding or cybersecurity knowledge needed.

Audience	Grades 6-8. No prior experience needed.
Time	About 60 minutes (5 minute opener, 45-50 minutes of missions, 5-10 minute wrap-up)
Student link	**codehscyberrange.com/hoc**
Mission passcode	**`secret-agent-72`**
Accounts	None. Students do not sign up or enter any personal information.
Materials	One computer or Chromebook per student (or per pair) with an up-to-date web browser.

Before the Hour of Code

- **Test it on a student device.** Open **codehscyberrange.com/hoc** on the same kind of computer and network students will use, enter the passcode, and open one activity. If the page is blocked, ask your IT team to allow **codehscyberrange.com**.
- **Try a mission yourself.** Playing the first activity takes about 10 minutes and is the best way to get comfortable before class.
- **Read the Teacher Notes** at the back of this guide. Each activity has an overview, objectives, discussion questions, and a step-by-step solution.
- **Write the link and passcode on the board** so students can get started right away.

During the Hour of Code

1. **Open with a question (5 minutes).** Ask: *"What do you think someone who works in cybersecurity does all day? Have you ever gotten a message or seen a website that seemed fake?"* Explain that today they will try the real work cybersecurity professionals do.
2. **Get students in.** Students go to **codehscyberrange.com/hoc**, type the mission passcode **secret-agent-72**, and click **Unlock your mission**. The passcode works on that browser for 24 hours.
3. **Students work at their own pace.** They open activities from the mission pathway in order. Each activity has a short story and directions, and a guide character walks them through every step.

4. **Capture the flag.** At the end of each activity, students unlock a career card with a flag that looks like **flag{...}**. They copy it, paste it into the **Found the flag?** box, and submit to clear the activity. Every student's flags are unique, so flags can't be shared.
5. **Keep everyone moving.** Most students finish the first five missions in about 45 minutes. The last five missions are a step up and take a little longer, so they work well for early finishers or a second session.
6. **Wrap up (5-10 minutes).** Bring the class together with the closing discussion questions below.

Closing Discussion Questions

- Which mission felt most like something you'd want to do as a job? Why?
- What is one thing you will do differently online after today?
- Many of these missions started with tricking a person, not a computer. Why do you think attackers do that?
- Which cyber career that you unlocked today surprised you most?

Hour of Code Tips

- **It's okay not to know the answers.** Every activity is designed for students with no background. Learning alongside your students is part of the fun.
- **Point students back to the guide.** When a student is stuck, ask them to reread the guide's last message and the directions before you step in. Wrong answers come with an explanation, not a penalty.
- **Use prompting questions** instead of giving answers: *What is the activity asking you to find? What clue have you not used yet? What would an attacker look for here?*
- **Progress is saved on the browser.** Students should use the same computer and browser for the whole session. Switching devices or clearing the browser starts them over.
- **Shared computers:** when a student is completely done, they can click **End mission & clear progress** so the next class starts fresh. Remind students not to click it mid-session.
- **Pair up if needed.** These activities work well with two students per device. Have partners switch who drives after each activity.
- **Everything is a safe simulation.** Students attack only fictional systems, and every activity reminds them that real hacking always requires permission.

Closing

Thank you for bringing cybersecurity to your students! We hope this hour sparks their curiosity about the many careers in cyber. If you have questions or feedback, reach out to us at **hello@codehs.com**.

Activity Overview

Activities appear on the mission pathway in this order. Times are estimates for a student working alone.

#	Activity	Topic	Career unlocked	Time
1	Crack the Vault	Web Security	Penetration Tester	8-10 min
2	Phish or Legit?	Web Security	Security Awareness Specialist	8-10 min
3	Secret Agent Decoder	Cryptography	Cryptographer	8-10 min
4	Night Shift at the SOC	Network Security	SOC Analyst	8-10 min
5	Digital Detective	Digital Forensics	Digital Forensics Investigator	8-10 min
6	Terminal Trainee	Linux	Threat Hunter	12-15 min
7	Hash Hunter	Cryptography	Security Engineer	12-15 min
8	Bug Bounty	Web Security	Bug Bounty Hunter	12-15 min
9	Coffee Shop Wi-Fi	Network Security	Network Security Engineer	15-18 min
10	Ransomware Rescue	Digital Forensics	Incident Responder	12-15 min

Teacher Notes: Activity 1

Crack the Vault

Web Security | About 8-10 minutes | Career unlocked: **Penetration Tester**

Overview

Students act as an ethical hacker hired by Coach Vega. They read her public posts to guess her password, compare passwords in a head-to-head showdown, then build their own password that would take at least 1,000 years to crack.

Objectives

Students will be able to:

- Explain how attackers use public information (OSINT) to guess passwords
- Explain why a long password beats a short one with symbol swaps
- Create a strong passphrase from several random words

Discussion Questions

- What clues about you could someone find online? Could any of them be part of a password?
- Why is purple-waffle-rocket stronger than P@ssw0rd!?
- What makes ethical hacking different from criminal hacking?

Solution

1. Read Coach Vega's posts and notice that her dog is named Pickles and that she was born in 1988.
2. Combine the two clues from the hint (best buddy's name + birth year) and enter Pickles1988 to open the vault.
3. In the Password Showdown, pick the longer passphrase in rounds 1 and 2, and pick the random 8-character password over the single dictionary word in round 3.
4. In the Password Lab, type a password made of 3 or 4 random words joined by dashes, such as purple-waffle-rocket, until the timer shows 1,000+ years, then click Lock it in.
5. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students experience both sides of password security: how attackers use public information (OSINT) to guess weak passwords, and why length beats symbol swaps when a computer can make billions of guesses per second. The activity introduces the penetration tester career and the idea that ethical hacking always requires permission.

Teacher Notes: Activity 2

Phish or Legit?

Web Security | About 8-10 minutes | Career unlocked: **Security Awareness Specialist**

Overview

Students sort six messages in Alex's inbox as phish or legit, then click the specific red flags in each phishing message, such as look-alike senders, fake deadlines, and requests for passwords or gift cards.

Objectives

Students will be able to:

- Define phishing and social engineering
- Identify common red flags in emails and texts
- Explain why a safe message can still be checked by opening the app directly

Discussion Questions

- Have you or someone you know ever gotten a message like these? What gave it away?
- Why do scammers try to make you feel rushed or scared?
- What should you do if a message from a friend seems strange?

Solution

1. Mark the GameVault Rewards email as Phish, then click the look-alike sender address, the 10 MINUTES deadline, and the request for your username and password.
2. Mark the school library email as Legit because it comes from the school address, uses Alex's name, and asks for nothing private.
3. Mark the ParcelPost text as Phish, then click the surprise fee, the 24-hour deadline, and the fake link.
4. Mark Jayden's text as Phish, then click the vague message, the shortened link, and the request to log in.
5. Mark the StreamFlix sign-in alert as Legit because it has no links and tells Alex to open the app directly.
6. Mark the Principal Davis email as Phish, then click the Gmail address, the gift card request, and the request to keep it secret.
7. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Most cyberattacks begin with a single message that tricks a person instead of a computer. Sorting real and fake messages, and naming the specific red flags, builds the habit of slowing down before clicking. It also introduces social engineering and the security awareness career.

Teacher Notes: Activity 3

Secret Agent Decoder

Cryptography | About 8-10 minutes | Career unlocked: **Cryptographer**

Overview

In spy training, students use a cipher wheel to decode a message from HQ, crack a rival spy's message without the key by trying every shift, and encrypt a reply.

Objectives

Students will be able to:

- Define encryption, decryption, and key
- Encrypt and decrypt a message with a Caesar cipher
- Explain why a cipher with only 25 keys is easy to break

Discussion Questions

- How long would it take a computer to try all 25 Caesar shifts?
- Where do you think encryption is used in your everyday life?
- What would make a cipher harder to crack?

Solution

1. Click + three times to set the wheel to Shift 3, then find H in the Normal row and enter the letter below it, K.
2. Keep the wheel on Shift 3 and decode FRGH LV IXQ by reading each letter from the Secret row back up to the Normal row, which gives CODE IS FUN.
3. For the intercepted message, keep clicking + until the decoder output turns into readable words, then choose the meeting place it names.
4. Set the wheel to Shift 5 and encrypt AGENT READY letter by letter to get FLJSY WJFID, then click Send to HQ.
5. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students practice encryption and decryption with a key, then discover why a Caesar cipher is weak: with only 25 possible keys, a brute force attack cracks it in seconds. This sets up the idea that modern encryption uses math strong enough to resist computers, and introduces the cryptographer career.

Teacher Notes: Activity 4

Night Shift at the SOC

Network Security | About 8-10 minutes | Career unlocked: **SOC Analyst**

Overview

On the night shift at a Security Operations Center, students find the IP address attacking the school, flag the three log events that show the attack, and write firewall rules that block the attackers without blocking the school's own traffic.

Objectives

Students will be able to:

- Define IP address, log, and firewall
- Spot a brute force attack in data
- Write firewall rules that stop attackers without blocking normal users

Discussion Questions

- Why would 487 failed logins from one place be a warning sign?
- Why not just block all traffic to stop the attack?
- Why do you think SOCs are staffed 24 hours a day?

Solution

1. In the alarm chart, click 203.0.113.66, the IP address with 487 failed logins, because that many attempts means a program is guessing passwords.
2. In the event log, click Suspicious on the successful admin login after 487 failed attempts.
3. Click Suspicious on the free_coins_generator.exe program installed on Library-PC-4.
4. Click Suspicious on Library-PC-4 sending 2 GB of files to 198.51.100.77 at 3:12 AM.
5. In the firewall, add a BLOCK rule for 203.0.113.66 and a second BLOCK rule for 198.51.100.77.
6. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students follow the detect, investigate, respond cycle that SOC analysts use: spotting a brute force attack in data, separating suspicious log events from normal activity, and writing targeted firewall rules. The trap options (blocking all traffic or the school's own server) show that good defense stops attackers without breaking things for everyone.

Teacher Notes: Activity 5

Digital Detective

Digital Forensics | About 8-10 minutes | Career unlocked: **Digital Forensics Investigator**

Overview

Someone hacked the school website. Students search a server log, look up an IP address, and read photo metadata to rule out suspects one by one and identify The Phantom.

Objectives

Students will be able to:

- Define metadata
- Use logs, IP lookups, and metadata as evidence
- Use evidence to rule out possibilities step by step

Discussion Questions

- What information might a photo you post reveal without you realizing it?
- Why was The Phantom's 'prank' still a crime?
- How did writing down a password help the hacker?

Solution

1. In the server log, click the 11:42 PM row where the webteam account ran EDIT index.html from IP 198.51.100.23.
2. Type 198.51.100.23 into the IP Lookup tool and see that it belongs to Riverside Public Library's guest Wi-Fi.
3. Rule out Max Chen and Jordan Diaz, because their alibis place them at home and on the team bus instead of the library.
4. Click the broccoli photo to view its metadata, which shows it was taken on a Nova X phone, then rule out Riley Brooks, who has a Pixelate 5.
5. Accuse Sam Okafor, who was at the library and owns a Nova X phone.
6. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students combine three kinds of digital evidence (logs, IP address lookups, and photo metadata) to narrow down suspects, just like a digital forensics investigator. The ending reinforces two lessons: written-down passwords are easy to steal, and hacking without permission is illegal even as a prank.

Teacher Notes: Activity 6

Terminal Trainee

Linux | About 12-15 minutes | Career unlocked: **Threat Hunter**

Overview

Students log in to a simulated Linux terminal and learn one command at a time (whoami, pwd, ls, cd, cat, grep, rm) to follow a hacker's trail, find a hidden file, and delete the backdoor they left behind.

Objectives

Students will be able to:

- Explain what a terminal is and why security professionals use one
- Navigate folders and read files with basic Linux commands
- Use grep to search a large file for a word

Discussion Questions

- Why might typing a command be faster than clicking through folders?
- Why would a hacker hide a file by starting its name with a dot?
- How did grep save time compared to reading the whole log?

Solution

1. Run whoami, pwd, and ls to see that you are the analyst account in /home/analyst with README.txt, logs, and messages.
2. Run cat README.txt, then cd messages, ls, and cat from_it.txt to learn that hidden files start with a dot.
3. Run ls -a in the messages folder, then cat .hacker_plan.txt to read Z3R0's plan.
4. Run cd .. and then cd logs, and try cat access.log to see that it is too long to read.
5. Run grep Z3R0 access.log to find the line saying Z3R0 hid .backdoor.sh in the logs folder.
6. Run ls -a to see the hidden file, then rm .backdoor.sh to delete it.
7. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students learn the core Linux commands for moving around a file system, reading files, finding hidden files, and searching with grep, using a guided story that gradually removes the scaffolding. The jump from scrolling 240 log lines to finding the answer with one grep command shows why security professionals rely on the terminal.

Teacher Notes: Activity 7

Hash Hunter

Cryptography | About 12-15 minutes | Career unlocked: **Security Engineer**

Overview

A website's password list leaked, but it stored hashes instead of passwords. Students experiment with a hash machine, spot two users with the same password, and run a dictionary attack that cracks five of six accounts.

Objectives

Students will be able to:

- Describe what a hash is and how it behaves
- Explain how a dictionary attack cracks hashed passwords
- Explain why a long, random passphrase survives a dictionary attack

Discussion Questions

- If hashes can't be reversed, how were five accounts cracked anyway?
- Why did two users having the same hash give away a secret?
- What makes rbrooks's password safe?

Solution

1. Hash cat twice to see it makes the same fingerprint, then hash Cat to see that one capital letter changes everything, then hash a sentence of 25 or more characters to see the fingerprint stays the same length.
2. Answer that hashes cannot be reversed, so attackers have to guess.
3. In the leaked list, click tnguyen and kpatel, who have identical hashes and therefore the same password.
4. Click words in the wordlist until soccer, password, letmein, and minecraft match, which cracks coach_vega, jsmith, principal_d, tnguyen, and kpatel.
5. Answer that rbrooks is safe because their long, random passphrase is not on the common password list.
6. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students discover the key properties of hash functions (they are repeatable, they scramble completely after a tiny change, they always have the same length, and they only work one way), then use those properties to run a dictionary attack. Seeing a long passphrase survive the attack, and spotting a shared password from matching hashes, explains why strong passwords and salting matter.

Teacher Notes: Activity 8

Bug Bounty

Web Security | About 12-15 minutes | Career unlocked: **Bug Bounty Hunter**

Overview

With the school's permission, students hunt for three bugs on a new grades website: a password left in the page source, a profile page anyone can view by changing the URL, and a hidden admin page listed in robots.txt. They pick the best fix for each.

Objectives

Students will be able to:

- Explain what a bug bounty program is and why permission matters
- Use View Source and the address bar to find web security bugs
- Choose an appropriate fix for each bug

Discussion Questions

- Why would a company pay people to find its bugs?
- Why isn't hiding a page the same as protecting it?
- What should you do if you find a bug on a site that doesn't have a bug bounty?

Solution

1. Click View Source and click line 6, the HTML comment containing the admin login, then choose the fix that deletes the comment and changes the password.
2. Change the address bar from /profile?id=105 to another number such as /profile?id=106 and press Go to see another student's grades, then choose the fix that checks the logged-in student owns the profile.
3. Visit /robots.txt to find the line Disallow: /secret-admin-panel.
4. Visit /secret-admin-panel to find an admin page with no login, then choose the fix that requires an admin login.
5. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students find three real and common web vulnerabilities: secrets left in source code, insecure direct object references (IDOR), and relying on robots.txt to hide a sensitive page. Picking a fix for each bug, and the reminder that bug bounties require permission, shows the responsible-disclosure side of ethical hacking.

Teacher Notes: Activity 9

Coffee Shop Wi-Fi

Network Security | About 15-18 minutes | Career unlocked: **Network Security Engineer**

Overview

At a cafe, students avoid a fake evil twin network, sort safe and unsafe pop-ups, use a packet sniffer to see what HTTP leaks compared to HTTPS, check URLs before logging in, and choose safe phone settings.

Objectives

Students will be able to:

- Explain the difference between HTTP and HTTPS
- Recognize an evil twin network and look-alike web addresses
- Choose device settings that make public Wi-Fi safer

Discussion Questions

- What can an attacker still see even when a site uses HTTPS?
- Why isn't the lock icon alone enough to trust a site?
- What settings will you check on your own phone after this?

Solution

1. Avoid the open BeanThere_Guest evil twin and choose the BeanThere_Guest network marked Secured, then enter latte4you from the sign.
2. In Pop-up Patrol, tap Accept on the cafe rules and Install tonight on the Settings update, and close the school-password sign-in, the virus warning, and the file from CoolKid_123.
3. In the packet sniffer, click the HTTP POST /login packet and enter the password tacoTuesday!, then click a green HTTPS packet to see that its contents are scrambled.
4. For Task 3, check the three website names from the DNS packets (quizgames.example, mail.lincolnms.example, and weather.example) and leave the email contents and email password unchecked.
5. Mark https://mail.lincolnms.example and https://www.wikipedia.org/login as OK, and mark http://quizgames.example/login, https://lincolnms-grades.login-check.co, https://lincolnms.example.secure-login.co/grades, and http://bean-there-wifi.example/verify-account as STOP.
6. Turn off Auto-join open Wi-Fi and Receive files from everyone, turn on Ask before joining networks, VPN, and Automatic updates, then click Save settings.
7. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students practice a full set of public Wi-Fi defenses and see that HTTPS hides what you send, but not which sites you visit.

Teacher Notes: Activity 10

Ransomware Rescue

Digital Forensics | About 12-15 minutes | Career unlocked: **Incident Responder**

Overview

Ransomware has locked a computer in the school office 45 minutes before school starts. Students contain it, find the phishing email that started it, find the other infected computers, restore from the right backup, and choose ways to prevent the next attack.

Objectives

Students will be able to:

- Define ransomware
- Follow the incident response steps: contain, investigate, recover, learn
- Choose a backup based on when an attack started

Discussion Questions

- Why is unplugging the computer the first move instead of paying?
- How did the attachment Invoice_URGENT.pdf.exe trick the user?
- Why should one backup copy be kept offline?

Solution

1. Choose to unplug the infected computer from the network to isolate it.
2. Click the Billing Dept email with the Invoice_URGENT.pdf.exe attachment, which is a program disguised as a PDF and arrived right before the 7:12 AM attack.
3. Inspect each computer and isolate Office-2 and Principal, whose files end in .locked and include a ransom note, while marking the clean computers as clean.
4. Restore from the Monday 6:00 AM backup, the newest one made before the attack started at 7:12 AM.
5. For lessons learned, choose phishing training, automatic updates, and keeping backups that include an offline copy.
6. Copy the unique flag from the career card, paste it into the Found the flag? box, and submit.

Why it matters

Students walk through the incident response lifecycle (contain, investigate, scope, recover, and learn) in a time-pressured ransomware scenario. Choosing a backup by comparing its timestamp to the infection time, and spotting a double file extension, connect this challenge to the phishing and forensics skills from earlier missions.