

Guardian Week 2: Spot the Attack, Plan the Exam

Mon, Dec 14 – Tue, Dec 15 · 2:30–4:00 PM · Room 105 (or live on Zoom; the link comes by email)

This week: Catch phishing and other tricks, learn the malware types, earn your sixth badge, and take Practice Exam 1 before winter break.

Heads up

- Last meetings before winter break. We return Monday, Jan 4.
- Over break: 10 minutes a day in the app keeps your streak and your memory alive. It's optional, and it counts.

Read-aheads

Before Monday (15 minutes)

- Read the Social engineering and Malware notes below.
- Look at the last 10 messages or emails you got. Would any of them fail the phishing checklist?
- Play one round of Phish Tank in the Arcade.

Before Tuesday (20 minutes)

- Read the Exam basics notes below.
- Finish the Guardian Study Path.
- Look at your badge list. Which zone was your hardest? Write it down for your pacing plan.

The missions

Monday, Dec 14 · Day 19

11A · Game Phish Tank Escape Room

Your crew is locked in the Phish Tank. To escape, sort 12 realistic messages into safe or phishing, spotting the tells: urgency, mismatched links, odd senders, and requests for passwords. Then identify smishing, vishing, shoulder surfing, and tailgating in four short videos.

1. Play Phish Tank and sort all 12 messages, writing the tell for each phishing attempt.
2. Watch the four social-engineering clips and name the attack type in each.
3. Draft a one-paragraph warning your crew could post to warn other students.

Turn in: Phish Tank score with tells listed, clip identifications, and the student warning paragraph.

Tuesday, Dec 15 · Day 20

Guardian Gate and Practice Exam 1. You must pass the Keeper Gate first.

11B · Exam prep Exam Strategy and Practice Exam 1

Tonight you learn how the real Tech+ exam works: question count, time, flagging, and pacing. Then you take the Guardian Gate for badge six and begin full Practice Exam 1 under timed conditions. Your score tells you exactly where to focus for the final two weeks.

1. Review the exam format and write a personal pacing plan for roughly one minute per question.
2. Take the 20-question Guardian Gate solo; 17 of 20 (85 percent) passes.
3. Begin timed Practice Exam 1 and finish any remaining questions before Meeting 12A.

Turn in: Pacing plan, each member's Guardian Gate result, and Practice Exam 1 score.

Notes

Social engineering

- Phishing: a fake message that tries to get you to click, log in or pay. Tells: urgency, a sender domain that's slightly off, a link that doesn't match, a request for your password or money.
- Smishing: phishing by text message. Vishing: phishing by voice call.
- Tailgating: following an authorized person through a locked door.
- Shoulder surfing: watching someone type a password or PIN.
- Rule: no real company or school will ask for your password by email, text or phone.

Malware and defenses

- Virus: attaches to files and spreads when they run. Worm: spreads across networks by itself.
- Trojan: looks useful but hides something harmful. Spyware or a keylogger secretly records what you do or type.
- Ransomware: locks your files and demands payment. Separate backups are the real defense.
- Adware: floods you with unwanted ads.
- Defenses: keep the OS and apps patched, run antivirus, keep the firewall on, use a VPN on public Wi-Fi, and review privacy settings.

Exam basics (CompTIA Tech+)

- Up to 70 questions in 60 minutes, so plan on less than one minute per question.
- Scores run from 100 to 900. Check the passing score with Mr. James before you book.
- Flag hard questions, answer every question (blanks are wrong), and come back to flags at the end.
- In the app: Exam Sim gives you a full-length practice run with a zone-by-zone review.

Vocabulary

Phishing	A fake message that tricks you into acting
Smishing	Phishing by text
Vishing	Phishing by phone call
Ransomware	Malware that locks files for payment
Trojan	Malware disguised as something useful
Firewall	Filters network traffic by rules

Check yourself

1. A text says your school account is locked and gives you a link. Which attack is this?
2. Someone slips into the server room behind a teacher. What is it called?
3. What gets a school's files back after ransomware without paying?

Answers: 1. Smishing 2. Tailgating 3. Recent backups stored separately from the infected machine.

Bring

- A charged device
- Your student ID card
- Your hardest-zone note for the pacing plan