Security Mad Libs

Fill in the blanks using the category shown, then read your story out loud.

Team Names: _____

Categories used in these stories: a name, a number, *a social engineering tactic*, *technical jargon*, *an adversary type*, and *a defense action*. The first round, try to give a real, correct answer for each vocab-category blank - see if the story reads as a genuinely plausible incident. Second round: go wild.

Story 1: The Office Breach

It started when _____ (name) in accounting got an email that looked like it came from the CEO. The email used _____ (a social engineering tactic) to make her feel like she had no time to think it through. Without checking, she clicked a link and typed her password into a fake page - a classic case of _____ (technical jargon). Three days later, the security team noticed _____ (technical jargon) in the login logs: the same account, logging in from _____ (a number) different countries in one hour. When they finally identified the attacker, records showed they were a _____ (adversary type) - not some elite mastermind, just someone patient enough to wait for the right moment. The fix? IT had to _____ (defense action) the account immediately, then require everyone in the building to _____ (defense action) before logging in again.

Story 2: The Late-Night Call

_____ (name) was almost asleep when the phone rang. The voice sounded exactly like their _____ (a family member), panicked, saying they needed _____ (an amount of money) sent immediately. It's a common attack now, thanks to a technique called _____ (technical jargon). The scammer used _____ (a social engineering tactic) to keep _____ (same name as before) from thinking clearly and calling anyone else first. Afterward, investigators traced the call back to a _____ (adversary type) operating out of a call center overseas. Security experts recommend everyone set up a _____ (defense action) - like a family safe word - so this kind of trick doesn't work twice.

Story 3: The Office Wi-Fi

During lunch, _____ (name) connected to a Wi-Fi network called "_____ (a silly wifi name)" without checking if it was real. It turned out to be a fake network known as a(n) _____ (technical jargon), set up by someone using a technique called _____ (technical jargon) to scan for victims nearby. Everything _____ (same name) typed for the next _____ (a number) minutes was visible to the attacker - a _____ (adversary type) just looking for an easy target, not

anyone especially skilled. IT's advice afterward: always _____ (defense action) before connecting to public Wi-Fi, and consider using a _____ (defense action) any time you're on a network you don't fully trust.

Story 4: The Password Problem

_____ (name) used the same password - "_____ (a silly password)" - for every single account, including the school portal and their _____ (a social media app). When one random shopping site got hacked, attackers tried that same password everywhere else using a technique called _____ (technical jargon). Within _____ (a number) minutes, they were inside _____ (same name)'s school account too. It wasn't even a sophisticated attack - just a _____ (adversary type) running an automated tool. The lesson every security team repeats: never reuse passwords, and always turn on _____ (defense action) wherever it's offered.

Story 5: The Insider

_____ (name) had worked at the company for _____ (a number) years before getting passed over for a promotion one final time. Bitter about it, they used their still-active login to quietly plant a _____ (technical jargon) set to trigger a week after their last day. When investigators reviewed the case, it turned out to be a textbook example of _____ (technical jargon) - someone with legitimate access, misusing it on the way out. The adversary wasn't some outside hacker at all - it was a(n) _____ (adversary type), the hardest kind to guard against because they already had the keys. IT's new policy: _____ (defense action) every departing employee's access immediately, and _____ (defense action) any code changes made in someone's final two weeks.

Story 6: The AI Impersonator

An email landed in _____ (name)'s inbox that read more smoothly and personally than any phishing attempt she'd seen before - no typos, no weird phrasing, just a friendly note referencing a real conversation from last week. It had been written using _____ (technical jargon), which is exactly why it worked so well. The email used _____ (a social engineering tactic) to make the request feel routine instead of suspicious. Later, a security researcher tried something different: they typed a message directly to the company's AI chatbot, attempting _____ (technical jargon) to get it to reveal instructions it was never supposed to share. Both incidents were traced back to the same small, patient group - clearly not a random troublemaker, but a well-resourced _____ (adversary type). The company's response: _____ (defense action) for every AI system on the network, and _____ (defense action) for any email requesting something unusual, even if it sounds completely normal.