



## Cyber Villain Card Deck

Grades 3–5 · 30-minute lesson · 9 villains + 3 power moves

### STRONG LOCK

*A key AND a secret password.*

### FIX THE HOLES

*Patch the roof before the storm.*

### SPOT THE TRICK

*Not every message is real.*

### What's Inside

- 9 Villain Cards — each villain has a real-world tactic, rewritten for grades 3–5
- 3 Power Move Cards — the defensive moves that stop the villains
- 1 Final Boss — teaches defense in depth (needs all three power moves)
- 1 Teacher Answer Key — color-coded, with a layered-defense teaching tip

### How to Use This Deck

Print pages 2–4 on card stock. Cut along the outer borders of each card. Students read a villain's trick and match it to the power move that stops it. Keep page 5 (the answer key) for yourself. This deck pairs with the ThreatMon Teacher's Guide — see that document for the full 30-minute lesson plan.



CYBER VILLAIN

## SCATTERED SPIDER

*The Sweet-Talker*

### THE TRICK

Impersonates the IT help desk over the phone. Urgently asks a worker to hand over their password so they can "fix an account problem" — but the call is fake.

*Which power move stops this trick?*



CYBER VILLAIN

## COZY BEAR

*The Silent Shadow*

### THE TRICK

Sneaks in with stolen passwords and hides inside a network for months. Reads private messages and steals secrets without ever setting off an alarm.

*Which power move stops this trick?*



CYBER VILLAIN

## LAZARUS GROUP

*The Crack-Finder*

### THE TRICK

Hunts for outdated software that hasn't been patched in years. When it finds a weakness, it slips through like a key in an unlocked door.

*Which power move stops this trick?*



CYBER VILLAIN

## FANCY BEAR

*The Guesser*

### THE TRICK

Runs millions of common passwords — "password," "123456," pet names, birthdays — against an account until one finally works. Weak passwords don't stand a chance.

*Which power move stops this trick?*



CYBER VILLAIN

## SANDWORM

*The Power-Cutter*

### THE TRICK

Attacks unpatched computers that control real-world systems — power grids, hospitals, water plants. Can shut down a whole city if those systems aren't kept up to date.

*Which power move stops this trick?*



CYBER VILLAIN

## VOLT TYPHOON

*The Hider*

### THE TRICK

Quietly takes over old home routers and internet equipment that nobody has updated. Waits there for months, ready to launch an attack whenever it wants.

*Which power move stops this trick?*



CYBER VILLAIN

## FIN7

*The Fake-Mailer*

### THE TRICK

Sends emails that look like normal invoices or shipping notices. Hidden inside the attachment is malware — the moment someone opens the file, the villain is in.

*Which power move stops this trick?*



CYBER VILLAIN

## LAPSUS\$

*The Smooth Talker*

### THE TRICK

Bombards workers with fake texts and notifications until someone gets tired and taps "approve" on a login they didn't actually make. One careless tap is all it takes.

*Which power move stops this trick?*



FINAL BOSS

## NATION STATE APEX

*FINAL BOSS*

### THE TRICK

*This boss needs ALL THREE power moves!*

## About the Final Boss

**Nation State Apex** doesn't match just one power move. The real biggest villains in cybersecurity use every trick at once — so defenders use every power move at once. This is called **defense in depth**. Play this card after students have beaten at least 3 other villains, and require the pair to name all three power moves and explain how each one helps.

**POWER MOVE****STRONG LOCK***A key AND a secret password.***WHAT IT IS**

Strong passwords + Multi-Factor Authentication (MFA).

**WHAT IT STOPS**

Villains who guess, steal, or trick people into giving up passwords.

**REAL DEFENDERS**

Real defenders use password managers and require a code from your phone when you log in.

**POWER MOVE****FIX THE HOLES***Patch the roof before the storm.***WHAT IT IS**

Keep software updated. Don't run old versions.

**WHAT IT STOPS**

Villains who sneak in through cracks in outdated programs or devices.

**REAL DEFENDERS**

Real defenders scan for "vulnerabilities" and patch them every week.

**POWER MOVE****SPOT THE TRICK***Not every message is real.***WHAT IT IS**

Check twice. If something feels off, ask a grown-up.

**WHAT IT STOPS**

Villains who send fake emails, fake calls, or fake online friend requests.

**REAL DEFENDERS**

Real defenders train their whole company to spot phishing. Some run fake phishing tests every month.

**How to Play**

1. One student draws a Villain Card and reads the trick out loud.
2. The other student picks the Power Move card that stops it.
3. Check the answer key. First to match 3 villains correctly wins the round.
4. Swap roles and play again. Save the Final Boss card for last.

## Villain → Power Move

Some tricks could technically be stopped by more than one move — the primary answer is listed.

VILLAIN	THE TRICK (short)	POWER MOVE
SCATTERED SPIDER	Fake IT help-desk calls	SPOT THE TRICK
COZY BEAR	Stolen passwords, stays hidden	STRONG LOCK
LAZARUS GROUP	Exploits old software	FIX THE HOLES
FANCY BEAR	Guesses weak passwords	STRONG LOCK
SANDWORM	Attacks unpatched systems	FIX THE HOLES
VOLT TYPHOON	Hides in old routers	FIX THE HOLES
FIN7	Fake email attachments	SPOT THE TRICK
LAPSUS\$	Tricks workers for passwords	STRONG LOCK
NATION STATE APEX	Uses every trick at once	ALL THREE

### Power Move Distribution

Strong Lock: 3 · Fix the Holes: 3 · Spot the Trick: 2 · All Three (boss): 1

#### TEACHING TIP · DEFENSE IN DEPTH

When a student picks the "wrong" power move, don't say they're wrong — ask them *why* they picked it. Often they've spotted a real secondary defense (e.g., MFA would help against phishing even if **Spot the Trick** is the primary answer). That's great thinking — it's the same reason the Nation State Apex boss card requires all three. Real defenders layer their defenses because no single move catches every villain.