2026 CORNCON CYBERSECURITY CONFERENCE



WHY THE FUTURE OF CYBERSECURITY STARTS IN CHILDHOOD



We cannot build a cyber-resilient society if we wait until adulthood to teach cyber judgment.

NIDHI SRIVASTAVA • CYBERSECURITY PROFESSIONAL • TEDx SPEAKER • AUTHOR • FOUNDER, DIGIARMORX

Staying secure in an increasingly complex and chaotic world

Start With a Child, Not a Hacker

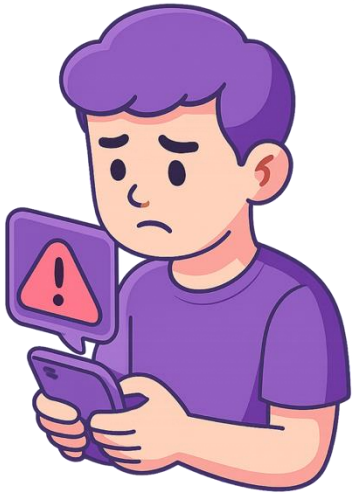
⚠ **YOUR GAMING ACCOUNT HAS BEEN REPORTED**

Verify your password now or your account may be deleted.

VERIFY NOW

Would a 10-year-old recognize the manipulation?

The cybersecurity threat landscape now lives inside games, group chats, school devices and children's everyday digital lives.



A Child's Digital World Today

Children become digital citizens long before they become employees.



GAMING

Online multiplayer • in-game chat • purchases

MESSAGING

Group chats • DMs • social platforms

SCHOOL PLATFORMS

EdTech apps • cloud accounts • shared devices

AI & CHATBOTS

AI tutors • assistants • generative AI

SMART DEVICES

Connected toys • tablets • wearables

DIGITAL PAYMENTS

In-app purchases • peer transfers

The Evidence Is Undeniable



95% **Teens Online**

of U.S. teens report daily internet access

Pew Research Center, 2024

7K+ **Sextortion Cases**

reports involving minors in 2023 alone

FBI IC3, 2023

46% **Cyberbullied**

of U.S. teens have experienced cyberbullying

Pew Research Center, 2025

79% **Data Shared**

of children's apps share data with third parties

Common Sense Media, 2025

The Attack Surface Has Moved

YESTERDAY

Yesterday

Network →
Device →
Application →
User



Today

Network →
Device →
Application →
→ User → Child
Child → Family
Family

THE PERIMETER HAS EXPANDED

Cybersecurity now depends on human judgment outside the enterprise — in homes, schools, and children's hands.

“The human layer cannot simply be patched.”

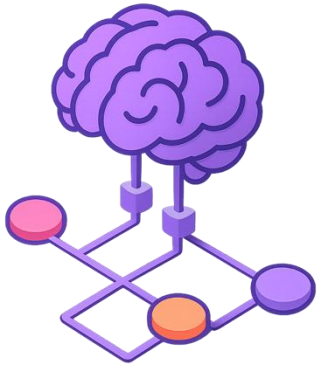
Children Are Not Small Adults

IMPULSE CONTROL	Still developing
RISK PERCEPTION	Online consequences can feel distant
SOCIAL VALIDATION	Peer approval can override caution
MANIPULATION DETECTION	Social engineering can be difficult to spot

WHY IT MATTERS

These developmental gaps can increase vulnerability to phishing, gaming scams, social engineering, deepfakes and oversharing.

Source: Steinberg (2014), Adolescence; UNICEF (2021)



The Education Gap



WE TEACH CHILDREN	DIGITAL SAFETY IS OFTEN
Mathematics	One annual assembly
Reading & Writing	One worksheet
Fire Safety	“Don’t click suspicious links”
Stranger Safety	

If the risk is daily, why is the education annual?

Knowledge ≠ Judgment

Cybersecurity education must build behavior and resilience — not vocabulary.

1	2	3	4	5
KNOWING	**RECOGNIZING**	**DECIDING**	**RESPONDING**	**RECOVERING**
“I know what phishing is.”	“This looks suspicious.”	“I won’t click — even if curious.”	“I know what to do next.”	“I made a mistake. I know how to get help.”

What Would You Tell a 12-Year-Old?



“Your best friend asks for a verification code. The profile photo and writing style look correct.”

A Send the code

B Ask a question only your friend would know

C Contact them through another channel

D Ignore it

E Tell a trusted adult

AI-generated impersonation makes “Does this look real?” an increasingly weak safety test. Teach verification behavior.

The Childhood Cyber Resilience Loop



RECOGNIZE

Identify threats and manipulation

PAUSE

Interrupt impulsive digital decisions

VERIFY

Confirm identity, information and requests

RESPOND

Take the protective action

RECOVER

Report, seek help and learn

RECOGNIZE → PAUSE → VERIFY → RESPOND → RECOVER ↺

A repeatable decision process children can carry into new technologies and new threats.

2026 CORNCON CYBERSECURITY CONFERENCE

Cyber Education That Grows With the Child

Cyber risk matures as children mature. Education must keep pace.

ELEMENTARY	MIDDLE SCHOOL	HIGH SCHOOL
• Passwords • Personal information • Safe gaming • Cyberbullying • Trusted adults	• Phishing • Social engineering • Digital footprint • Privacy • AI-generated content	• Identity theft • Deepfakes • AI manipulation • Financial fraud • Cyber ethics • Career pathways

Seven Things Schools Can Start Tomorrow



01 **Replace annual lessons with short recurring learning**

02 **Use realistic scenarios, not definitions**

03 **Include AI and deepfake literacy**

04 **Measure decisions, not only quiz scores**

05 **Practice reporting and recovery, not just avoidance**

06 **Involve parents as partners**

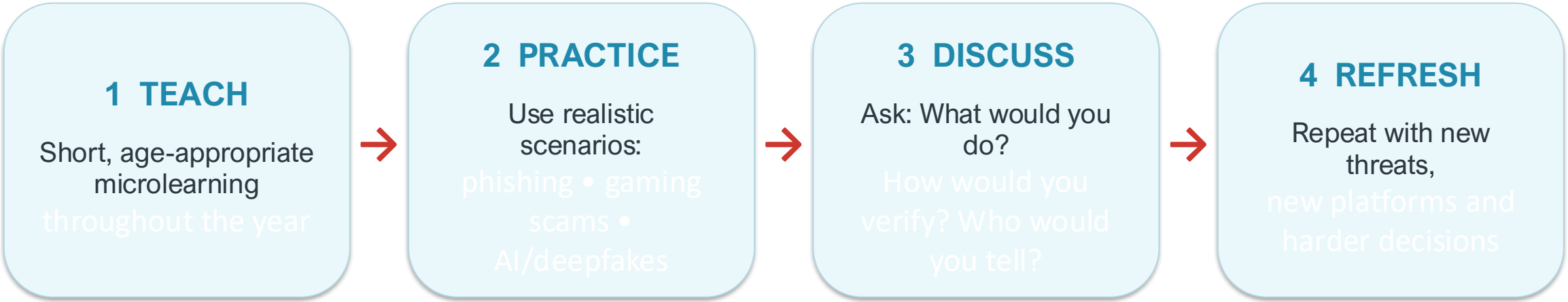
07 **Update scenarios as threats evolve**

Make cyber safety a continuous practice cycle — not a one-time assembly, worksheet, or annual compliance lesson.

2026 CORNCON CYBERSECURITY CONFERENCE

Cyber Safety Cannot Be a One-Time Lesson

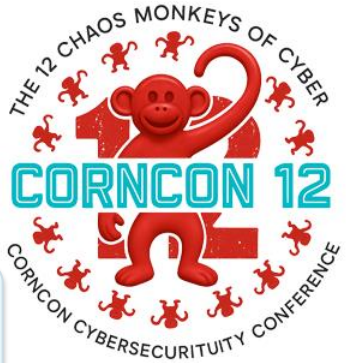
Threats change. Children grow. The learning cycle has to continue.



- Monday: show one suspicious message and let students identify the red flags.
- Monthly: run a 10-minute scenario on phishing, cyberbullying, privacy, gaming or AI.
- Quarterly: increase complexity and practice reporting + recovery, not just avoidance.
- After a new threat or platform trend: refresh the scenario instead of waiting for next year.

The goal is not one perfect lesson. It is repeated practice until safer decisions become a habit.

What Parents Can Do Tonight



ASK, DON'T JUST MONITOR

Ask "What happened online today?" — not only about screen time.

NO-PUNISHMENT RULE

Make it safe to report mistakes. Shame can lead to silence.

PRACTICE ONE SCAM

Role-play: "What would you do if…?"

TEACH PAUSE → VERIFY

Use it before clicking or responding to urgent requests.

CREATE A FAMILY RESPONSE PLAN

Know what to do for compromised accounts, cyberbullying and scams.

A Call to Cybersecurity Professionals

Extend your expertise beyond the enterprise.

“The next generation of cybersecurity professionals is already online.”

- → Volunteer in schools
- → Translate real threats into child-friendly scenarios
- → Mentor young cyber learners
- → Partner with educators — don’t expect them to become security experts
- → Include families in resilience conversations



The Big Shift

FROM		TO
Cyber awareness	→	**Cyber resilience**
Memorizing rules	→	**Practicing decisions**
Annual training	→	**Continuous learning**
Fear	→	**Confidence**
Protecting children from technology	→	**Preparing children to navigate technology safely**

Why I Care

“If cybersecurity professionals understand these threats why aren’t we translating that knowledge for children before they encounter them?”

As a cybersecurity professional and mother, I saw the gap firsthand when my own child experienced an online scam and cyberbullying. That moment became a larger mission.



Parents cannot monitor every message. Schools cannot predict every threat. Children need judgment they can carry with them.

Apply What You Have Learned Today

Turn childhood cyber resilience into action — immediately and repeatedly.

TOMORROW

- Use one realistic child-focused cyber scenario.
- Teach: Recognize → Pause → Verify → Respond → Recover.

NEXT WEEK

- Run the 10-Minute Cyber Resilience Challenge with a child, class, or family.
- Replace one definition-only lesson with decision-based practice.
- Make reporting mistakes safe: encourage a no-punishment response.

FIRST 3 MONTHS

- Build recurring, age-appropriate practice — not one annual lesson.
- Include phishing, gaming scams, cyberbullying, AI/deepfakes and privacy.
- Measure decisions and recovery behavior; involve parents and refresh scenarios as threats evolve.

If the risk is daily, the practice must be recurring.



Cybersecurity should not begin with an employee's first security training.

It should begin with a child's first digital decision.

RECOGNIZE • PAUSE • VERIFY • RESPOND • RECOVER

"The future of cybersecurity is already online — and many of them are children."

Nidhi Srivastava • Founder, DigiArmorX • www.digiarmorx.ai

Staying secure in an increasingly complex and chaotic world

Turning Cyber Resilience Into Practice

DIGIARMORX

AI-powered cybersecurity, digital safety and AI literacy education designed for K–12 learners.

STORIES | **ADAPTIVE** | **SCENARIOS** | **GAMES** | **DECISIONS**

Phishing & scams • Privacy • Cyberbullying • Gaming & social safety • Deepfakes & AI literacy • Cyber decision-making

digiarmorx.ai

2026 CORNCON CYBERSECURITY CONFERENCE

LET'S STAY CONNECTED

Continue the conversation on childhood cyber resilience, digital safety and AI literacy.

LINKEDIN	**Nidhi Srivastava** linkedin.com/in/nidhi-srivastava-a5493468
YOUTUBE	**@digiarmorxcyberkids** youtube.com/@digiarmorxcyberkids
INSTAGRAM	**@digiarmorx** instagram.com/digiarmorx
WEBSITE	**DigiArmorX** www.digiarmorx.ai
EMAIL	**Let's connect** learn@digiarmorx.ai

SCAN TO EXPLORE
www.digiarmorx.ai

Cyber risk follows the child. Cyber resilience should too.