Raising Discerning Digital Citizens

Trust, Safety, and Judgment in the Age of AI

Meet the Expert: Tina C. Williams-Koroma

- **Founder & CEO** of **TCecure** (Cyber services) and **CyDeploy** (Tech product for change impact).
- Over two decades in the **cybersecurity** field, including **leadership** roles at **Lockheed Martin** and **Unisys** protecting **critical infrastructure**.
- Background in **Computer Science, Management, and Law** (Esq., CISSP, PMP).
- **Passion:** Engaging with kids and guardians to ensure responsible, safe technology engagement and demystifying cybersecurity for families.

‘Sharenting’: Weaponizing Familiarity

The Data Trail: Parents often post birth dates, school locations, and milestones publicly.

The Con: Bad actors use this ‘99% truth’ to build instant trust with a child.

Predator: “I know your mom, Tina. We met at your **birthday** party at Chuck E. Cheese last November.”

The Rule: If you wouldn’t tell a stranger on the street, don’t post it publicly.

Weaponized Familiarity: The ‘Sharenting’ Risk

Social Post **Hacker Dossier**

- Public posts provide the '99% truth' attackers need.
- Predators feign intimacy: "I was at your 5th birthday party at Chuck E. Cheese."
- Data Permanence: A childhood photo becomes a security breach.

The New Threat Landscape: AI & Deepfakes

Social Media Photo

Deepfake Persona Synthetic Image

The Capability

Generative AI tools (like Grok or image generators) can create convincing personas or explicit images from innocent photos.

The Impact

Reports from the Internet Watch Foundation (IWF) and Childlight show a surge in AI-generated material. Even non-sexual images can be manipulated by AI.

The Risk

Predators use these tools to feign familiarity or for "sextortion"—blackmailing youths with fake or real images. Seeing is no longer believing.

The Core Challenge: Trust Has Been Redefined

The Old World

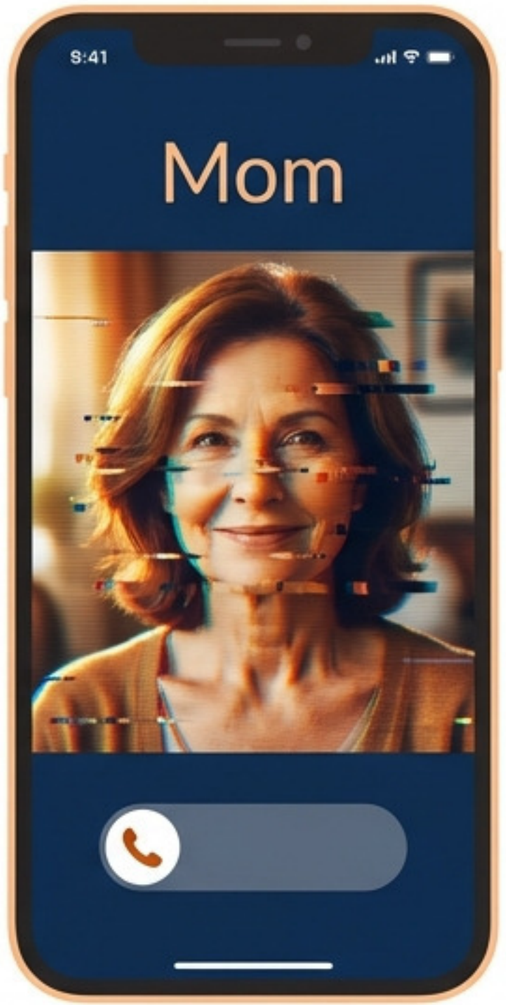
The New Reality

The Old Rule:
"Stranger Danger" worked because threats often **looked threatening.**

The Insight: The **worst lie** is one that is **99% true.** **Children need help spotting the 1% that is false.**

The New Reality:
Adversaries manufacture familiarity. **AI can fake voices, faces, and personas.**

Navigating the AI Age: Deepfakes & Voice Cloning



The Reality: AI can convincingly clone a loved one's voice or face.

The Family 'Safe Word': Establish a code word that only your family knows. If a call is distressing or suspicious, ask for the word.

Critical Thinking: If content creates a strong emotional reaction (fear, anger), pause. AI is designed to bypass logic by triggering emotion.

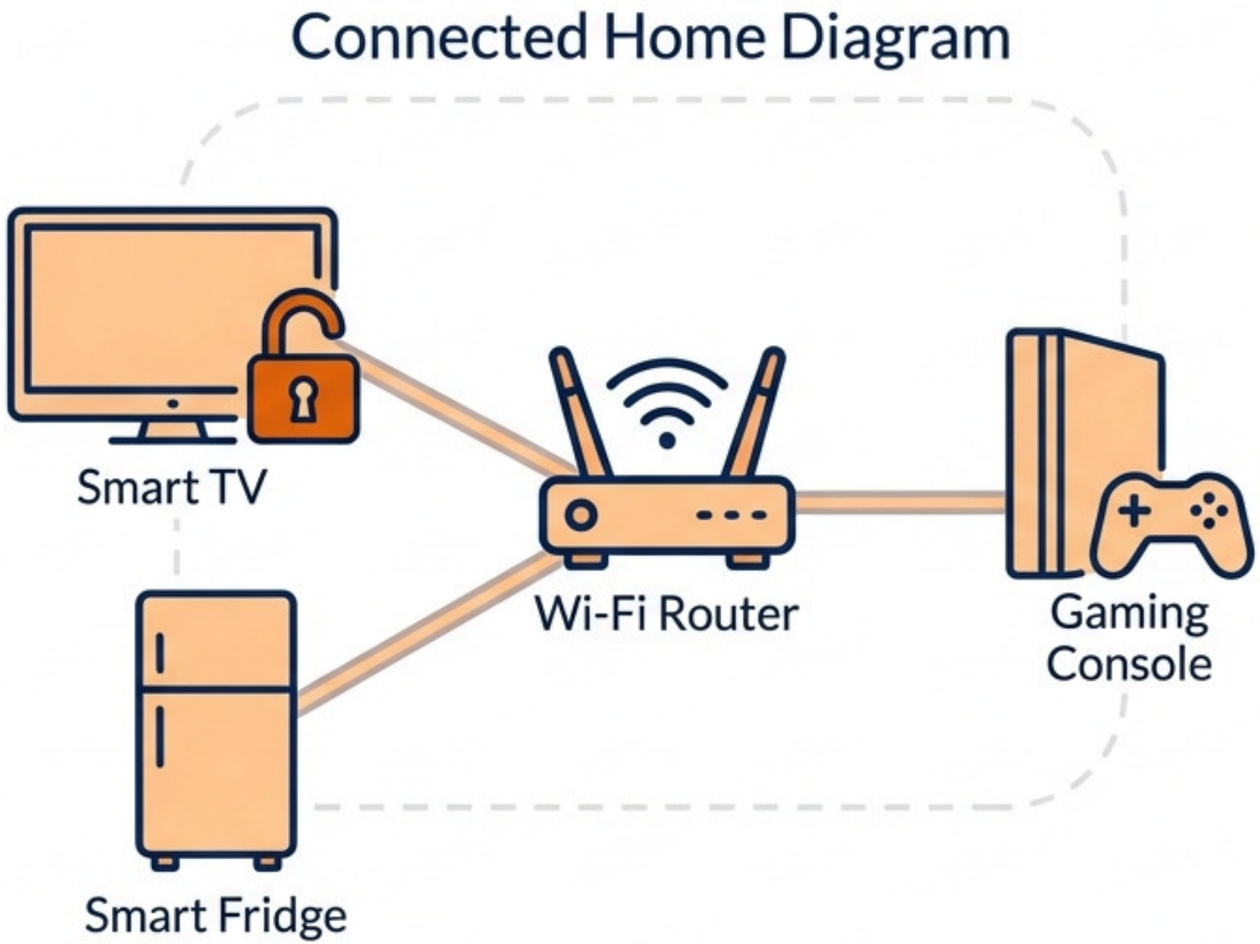
The ‘Trojan Horse’ in the Playroom

Trouble in Toyland 2025 Findings:

- U.S. PIRG Education Fund found that AI-enabled toys (like the ‘Kumma’ bear) can engage in unscripted, inappropriate conversations.
- In tests, toys provided advice on “being a good kisser,” engaged in roleplay scenarios involving spanking, and discussed weapons.
- **The Privacy Gap:** These devices often collect biometric data (voice prints, facial scans) without robust security.

Action: Treat smart toys like open web access. Check privacy settings immediately.

The Invisible Intruder: Residential Botnets



What is it?

Residential Proxies (like the massive BADBOX 2.0 operation) hijack consumer devices—Android TV boxes, smart plugs, and routers—to route cybercrime traffic.

The Scale:

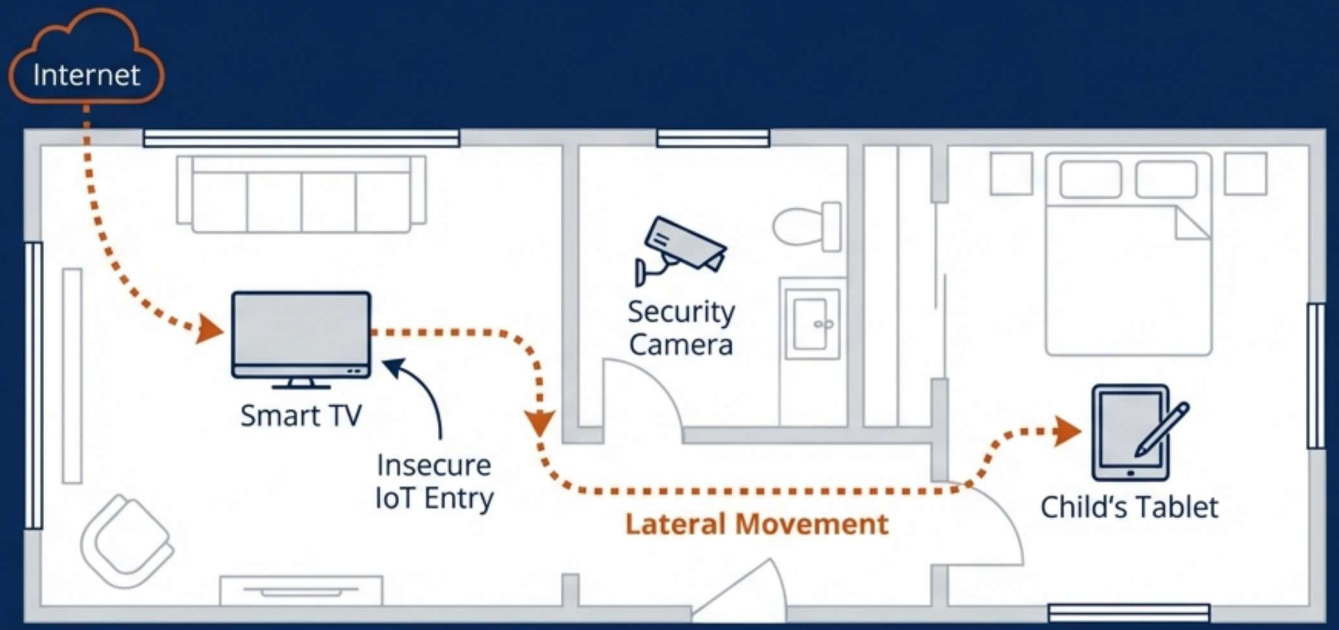
BADBOX 2.0 infected millions of devices in over 200 countries, turning homes into unwitting accomplices in fraud and data theft.

Based on public cybersecurity research and reporting on the BADBOX 2.0 botnet.

The Risk:

If a hacker controls your router or smart TV, they are effectively "inside the house." The same vulnerability that allows a botnet in can expose your child's data or location.

The “Digital Babysitter” Risk



The same mistake that compromises your router compromises your child.

Securing the Home Front: Digital Hardening

Guest Networks: Isolate smart toys and IoT devices on a separate ‘Guest’ Wi-Fi network.

Zero Trust at Home: Change all default passwords on cameras and routers immediately.

Updates: Keep firmware and software updated to patch vulnerabilities.

Privacy Audit: Turn off voice recording, location tracking, and camera access on apps and toys if not needed.

Shifting the Strategy: Monitoring vs. Mentoring

The Old Strategy

Monitoring, Banning, Restricting.

Effective only temporarily.
Impossible to sustain 24/7.

The New Strategy

Equipping Discernment.

Teaching the child to ask the right questions.

Analogy: We don’t carry children across the street forever; we teach them to look both ways.

The DISCERN Model: A Checklist for Trust (Part 1)

D 

D - Do I know them in real life? Have I met them face-to-face with a **parent present**? If not, they are a **stranger.**

I 

I - Information Source? How do they know my name or team? Could they have found it on a public post?

S 

S - Secret or Urgent? Are they asking me to keep secrets? Are they pressuring me to act fast? (Major Red Flags).

The DISCERN Model: A Checklist for Trust (Part 2)

C 

C - Check with an Adult. “Trust but verify.” Always clear new online contacts with a guardian.

E 

E - Emotions. Does this interaction make me feel scared, uncomfortable, or overly flattered?

R 

R - Real Friend Test. Would a real friend ask for this photo? Would a real friend ask for money?

N 

N - No means No. Do they respect my boundaries? If I say ‘no’, do they stop or push harder?

Applying DISCERN: Scenario Practice

Scenario A

The Situation: A “friend” online asks for a photo “just for me.”

The Filter: Apply **R** (Real Friend) and **S** (Secrecy).

Result: Real friends don’t ask you to break safety rules or keep secrets from parents.

Scenario B

The Situation: Someone knows your birthday and pet’s name.

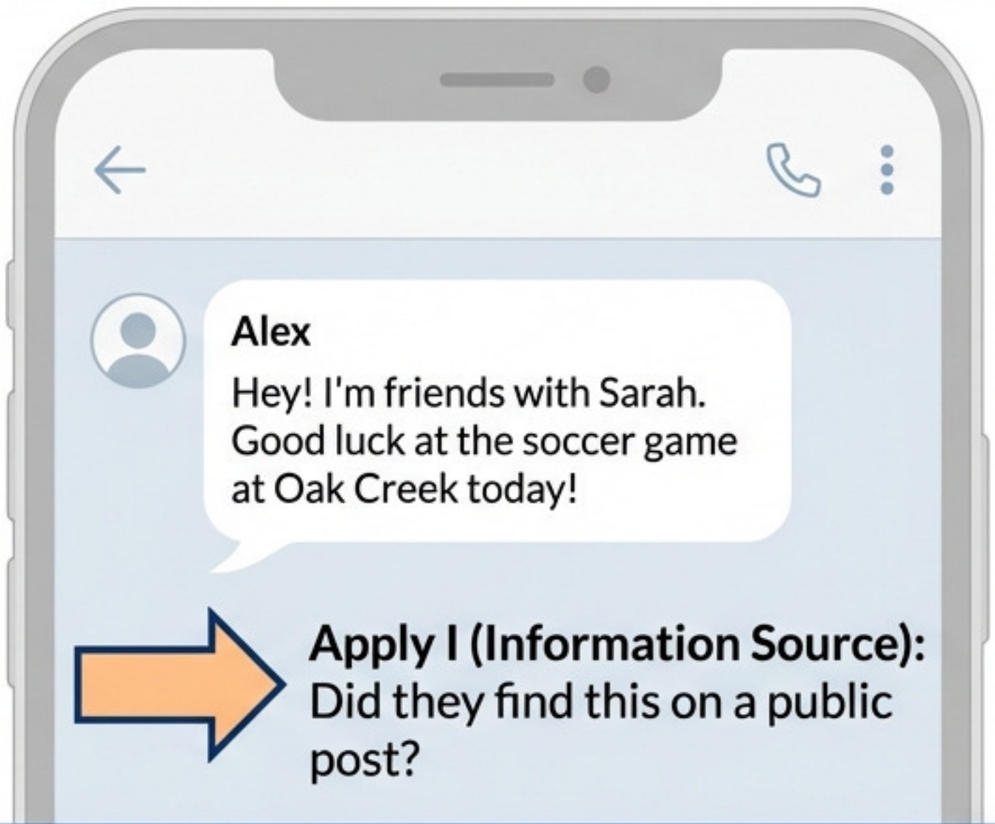
The Filter: Apply **I** (Information).

Result: Did they learn this from a public post? This is the “99% truth” deception.

If it can’t be checked offline and shared with a parent, it isn’t safe.

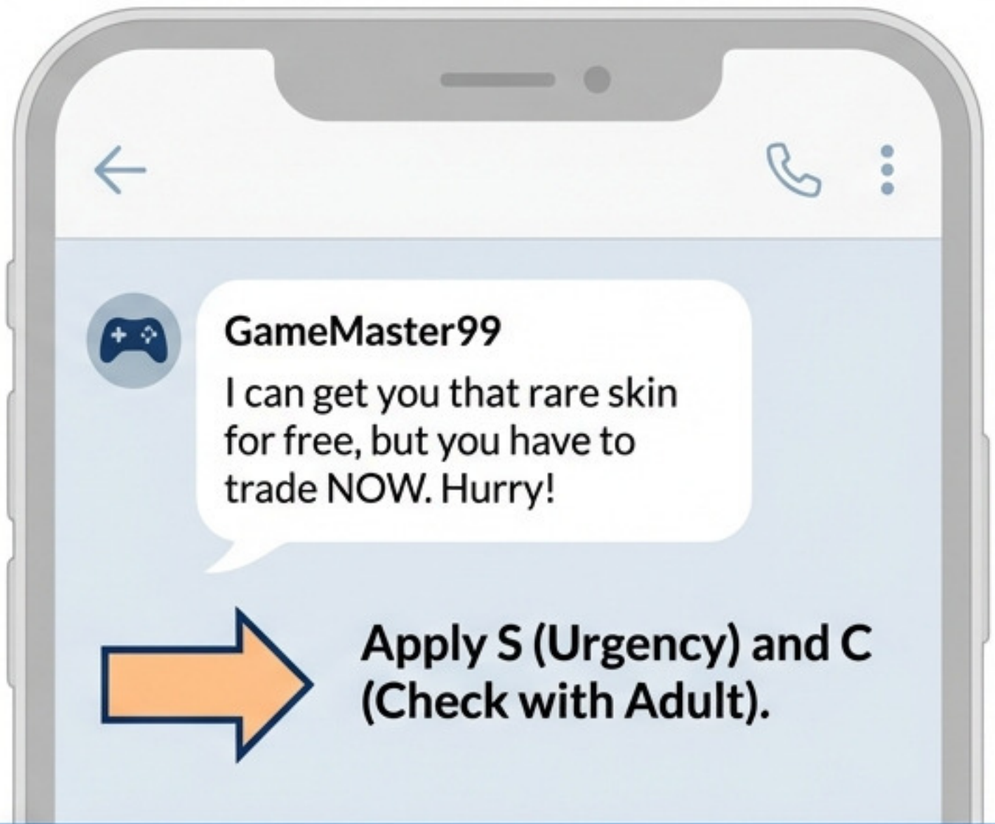
Practice Makes Perfect: Roleplay Scenarios

Scenario 1: **Personal Details**



Apply I (Information Source): Did they find this on a public post?

Scenario 2: **Urgent Offer**



Apply S (Urgency) and C (Check with Adult).

The Golden Rule: Never punish a child for disclosing a mistake. If they fear punishment, they will hide the problem.

A Framework for Balance: The 5 Cs

Source: NTIA / Center of Excellence on Social Media and Youth Mental Health

Child

Know your child's specific temperament and vulnerabilities.

Content

Focus on quality of engagement, not just quantity of time.

Calm

Do not use screens to soothe big emotions; build internal regulation.

Crowding Out

Ensure tech doesn't displace sleep, physical play, and connection.

Communication

Maintain open, non-judgmental dialogue.

A Trauma-Informed Approach

Informed by established trauma-informed care frameworks, including guidance from SAMHSA.

Context: Children in out-of-home care or with a **history** of trauma may be more vulnerable to "digital belonging" and online grooming.

Harm Minimization: Avoid punitive bans which drive behavior underground. Focus on relationship building.

Key Message: "You can always come to me, even if you made a mistake. I am your help, not your judge."

1. Redefine Trust: Online familiarity is not friendship.

3. Stop Sharenting: Protect the data that fuels deception.

2. Secure the Home: Segment networks to stop botnets.

4. Equip with DISCERN: Replace fear with judgment.

We cannot build a wall around the internet, but we can build a filter within the child.

The Goal: Resilience, Not Restriction

We cannot ban our way to safety.
The digital world is here to stay.

By combining open communication (The 5 Cs), practical tools (DISCERN), and technical safety (Hardening), we empower our children.

“The best filter is the one between their ears.”

Thank You

TCecure
Our Eyes Where You Need Them

CyDEPLOY

TCecure: Your Dedicated Cybersecurity Partner. Helping organizations build and maintain effective cyber programs.

CyDeploy: Understanding the impact of technology changes. An automated platform for testing security updates.

Contact us for more information.