



Stopping Digital Crime Before It Reaches Arkansans

A Practical State-Level Approach to Protecting Children and Seniors

Mission: Make the Internet Safe for People



- 20 years of experience identifying and stopping digital crime and harm.
- Monitors websites, apps, and digital advertising to detect malicious content, scams, and unwanted activity.
- Combines threat intelligence and human expertise to detect threats and enforce safety policies.
- Work with companies such as Walmart, Amazon, Microsoft, and Disney to protect their audiences and businesses.



- Identifies digital threats targeting children, seniors, and the vulnerable.
- Uses controlled simulations and AI personas to detect predators engaging victims.
- Combines detection, disruption and education to turn findings into **reduced crime and harm**.
- Works alongside existing web filters and cybersecurity tools.
- Commonwealth of Virginia, Erickson Senior Living, City of Carmel IN, Boys & Girls Clubs

THE REALITY: DIGITAL HARM & CRIME IS GROWING FASTER THAN ENFORCEMENT



- Americans spend **8–15 hours** per day online
- Digital platforms are now the **primary environment where crime occurs**
- Targeting: 39% of digital crime is seen at only one location
- Less than 1% of digital crime is ever pursued
- Most enforcement begins after victims harmed
- **\$300 billion financial loss** (FTC)
- Reported sextortion is **up 248% YoY**; suicide rate **up 40%** since 2000 (NCMEC)



Problem 1: What is Digital Harm?

PROBLEMS KIDS FACE VIA DIGITAL CRIME AND HARM

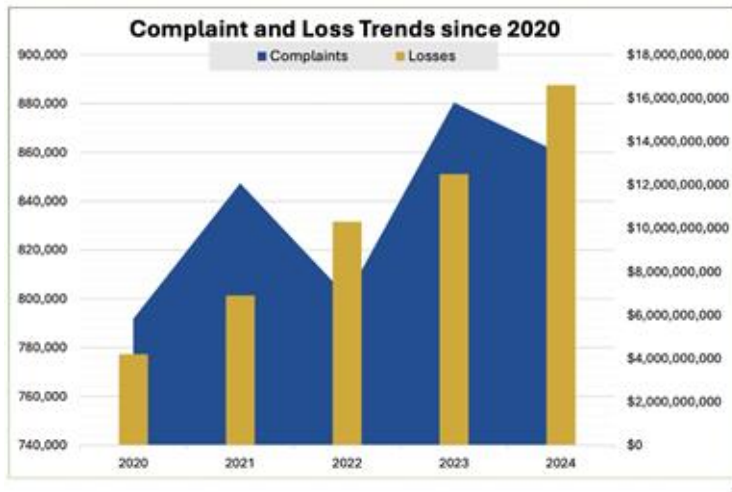
- Grooming and sextortion
- Drugs, alcohol, vaping
- Sexualization
- Mental health distress
- Social Media Addiction
- Human trafficking
- Gambling addiction
- Exposure to violence and indoctrination

PROBLEMS SENIORS FACE VIA DIGITAL CRIME AND HARM

- Financial devastation
- Psychological distress
- Health and wellness
- Medicare fraud
- Unsafe or fake products
- Personalized deepfakes
- Romance scams
- Loss of confidence
- Anxiety, depression, and shame

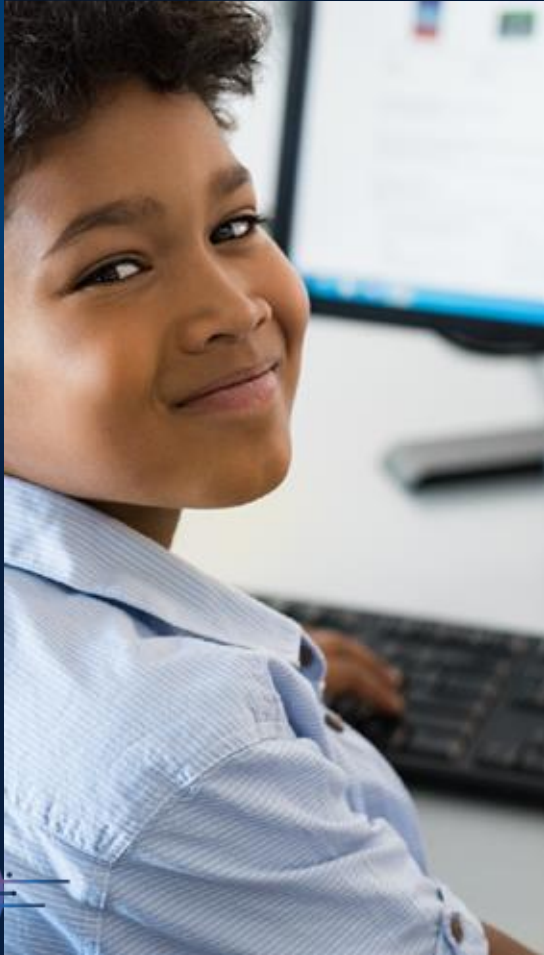


Problem 2 - ISSUES PERSIST WHEN THE PROBLEM IS NOT DIRECTLY ADDRESSED



- Cybersecurity, a \$750b industry – but is not protecting people
- Privacy, a \$250b industry – but is not addressing safety
- Legislation and regulation is largely unenforced
- Law enforcement pursues only .1% of the crimes
- Victim and mental health support is too late
- Education is good, but insufficient
- **WHAT IS MISSING?**

Deployment in AR school reveal digital threats and opportunities to stop them



- **Sexual and Violent Content Delivery**
Proxyware detected and stopped explicit content being immediately displayed without age verification.
- **Tobacco, Vaping, and Drug Promotion**
Proxyware detected and stopped tobacco and vaping ads plus drug-related websites served through mainstream ad networks.
- **Malicious Advertising Targeting Minors**
Proxyware detected and stopped cloaked creatives disguised as student tools and games.
- **Gambling and Prize Promotions**
Proxyware detected and stopped gambling content targeting kids, including methods that bypass web-filter and parental controls.

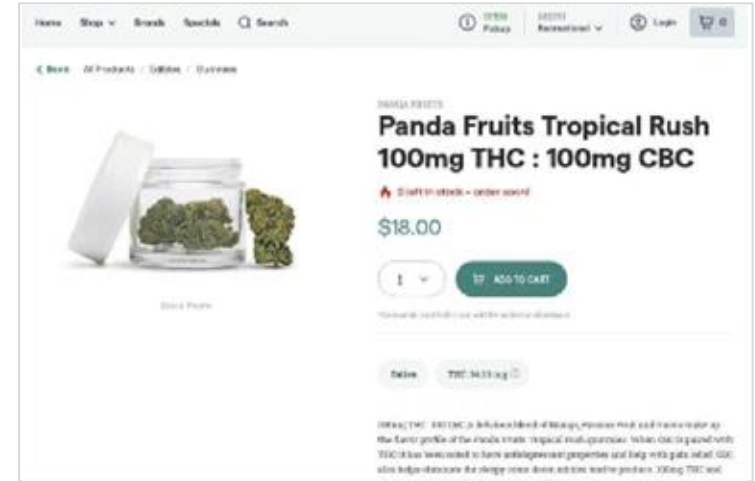
< > VAPING & DRUG ADDICTION

WHY IT MATTERS

- Introduces age-restricted products into children's everyday online experiences.
- Can normalize substance use and minimize perceptions of harm.
- Creates a direct pathways to purchase illegal products.

OPPORTUNITY

- Disrupt online promotions that connect children to vaping products and drugs.
- Reduce opportunities for underage purchases and early substance use.
- Help prevent addiction and reduce public spending on treatment and recovery.



Drug-related landing page accessible without age checks



Vaping ad served through mainstream ad network

< > ADULT CONTENT ACCESS AND SEXUALIZATION

WHY IT MATTERS

- Exposes children to explicit material they may not be prepared to understand.
- Introduce distorted portrayals of consent and sexual behavior.
- Can occur unexpectedly, without children actively seeking the content.

OPPORTUNITY

- Enforce Age Verification Laws
- Reduce child exposure to adult content
- Help reduce sexual violence and mental health issues due to under-age sexualization



Immediate display of explicit content with no identity verification "I am 18" click-through gates. Additionally, no geographic enforcement in age-protected state.

< > CHILDREN ARE ILLEGALLY TARGETED

WHY IT MATTERS

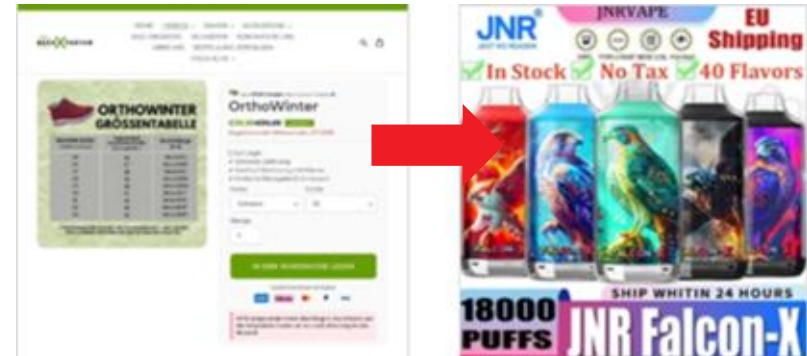
- Cloaked ads conceal a pathway to age-restricted products.
- Profile-based targeting exposes children to content adults reviewing the ad might never see.
- Intermittent redirects make the harmful behavior harder to detect.

OPPORTUNITY

- Uncover harmful ads and content shown to children but hidden from adults.
- Disrupt child access to illegal products.
- Provide evidence to hold deceptive advertisers accountable.



These products are shipped from Europe without age verification, creating a direct purchasing pathway for children.



< > GAMBLING ADDICTION IS RISING

WHY IT MATTERS

- Uses appealing prizes to encourage participation and disclosure of personal information.
- Introduces children to gambling creating lifetime addiction
- Apps supplied by bad actors may contain malware, creating ongoing access to a child's information and activity.

OPPORTUNITY

- Help prevent early gambling habits and reduce the risk of addiction.
- Expose giveaways that bypass parental controls or introduce malware.
- Reduce potential costs to families and public treatment and support services.



This \$500 bonus offer and casino loss incentives encourage online gambling, and bypasses age restrictions.



Electronics prizes encourage participation in sweepstakes and games.



< > GROOMING AND DECEPTION

WHY IT MATTERS

- Exploits children's trust in resources that appear educational, useful, or fun.
- Turns routine homework and gaming activity into opportunities to install malware and grooming data collection.
- Creates access for continued surveillance, targeting, and exploitation.

OPPORTUNITY

- Disrupt predatory contact before it escalates into coercion or sextortion.
- Equip schools and families with early warning signs and practical prevention tools.
- Give state agencies local crime intelligence to support investigations and coordinated action.



Fake homework helper redirected students to malware.



Fake Minecraft tool redirected students to malware.

A REAL-WORLD SEXTORTION SIMULATION



AI-generated synthetic personas deployed through multiple school communities reveal threats earlier, strengthen prevention, and provide law enforcement and policymakers with actionable local intelligence.

WHY WE DO IT:

To understand how online predators initiate contact and escalate toward sextortion, identifying warning signs before a young person is harmed.

HOW WE DO IT:

Deployed three AI-generated personas, ages 18–19, through a participating school's Wi-Fi, simulating typical social activity without involving real students.

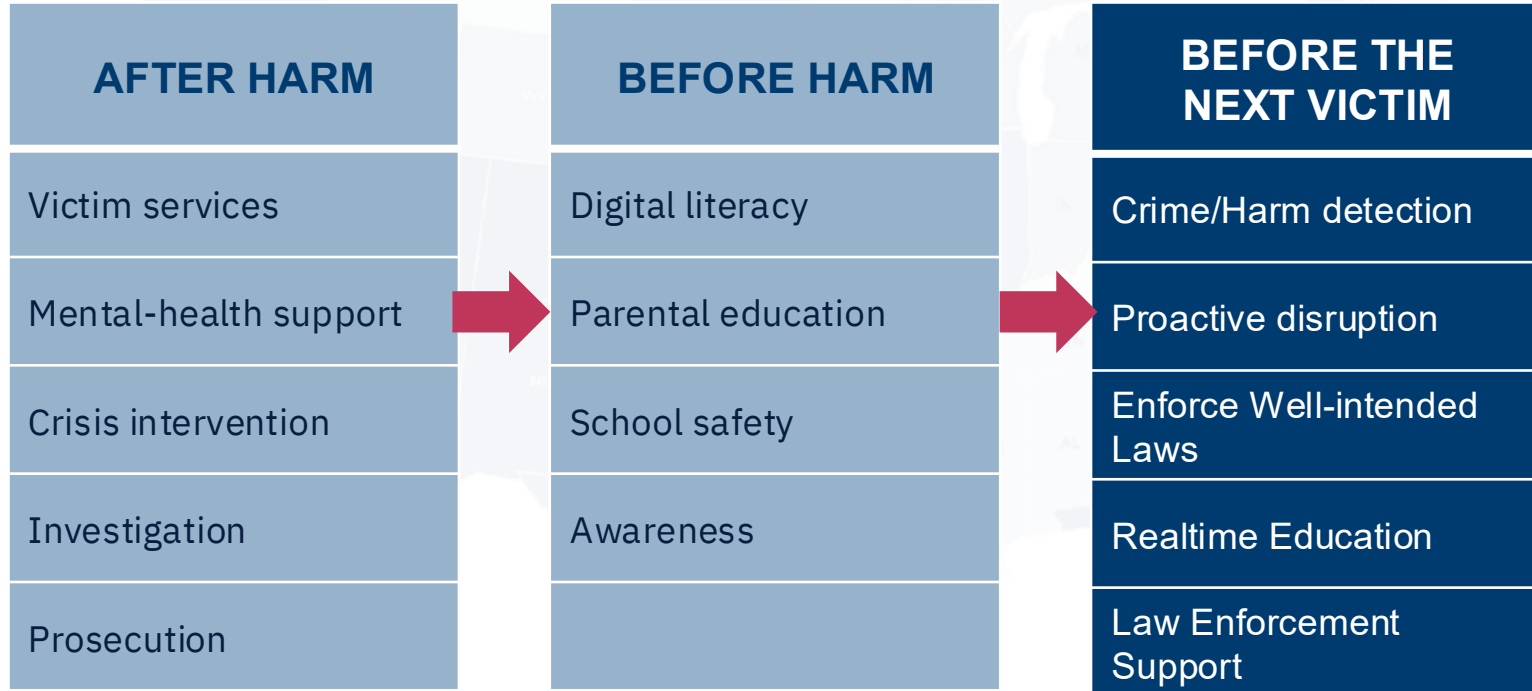
RESULTS:

Unsolicited contact began within approximately four weeks. Researchers documented escalating personal questions, photo requests, romantic pressure, and movement to private messaging, revealing opportunities for earlier detection and prevention.



A NEW APPROACH TO DIGITAL THREAT PREVENTION

The national focus on youth online safety creates an opportunity to think differently about where prevention begins.



*Many investments address the consequences of digital harm. Others help communities prepare for it. What is needed: detect the threat **BEFORE** the next child becomes the victim.*

SUCCESS IN VIRGINIA

5 SCHOOLS, 8 SENIOR LIVING COMMUNITIES

- 93% success rate of identifying and removing digital harm in participating schools
 - 77% of harmful online content blocked before reaching children
 - Sextortion Predator removed from Social Media Platform
-
- Senior cyber crime grew nationally by 43% while in Virginia it was cut to 13%.
 - Year 1: \$20M+ prevented from online fraud at participating senior living communities in Virginia
 - Year 2: Pacing for \$35.5M by the end of this year (207X ROI)
 - 40M+ digital attacks blocked targeting military and veterans

HOW TO FULFILL THE SETTLEMENT'S INTENT

THE MANDATE

Arkansas is set to receive \$172.4 million specifically designated to mitigate digital harms, curb social media addiction, and safeguard youth online.

THE LEGACY TRAP

If these funds are directed solely into mental health and static classroom lectures or broad awareness campaigns, we repeat past mistakes: teaching kids and seniors what to avoid without giving them the tools to defend against dynamic, automated threats.

THE TACTICAL OPPORTUNITY

Deploying funds toward active, technical threat detection and disruption immediately neutralizes threats and directly protects children and seniors—fulfilling both the letter and the spirit of the settlement.





CHRIS OLSON

CEO

The Media Trust & Proxyware

Chris@TheMediaTrust.com