CSNP
CYBERSECURITY NON-PROFIT

Family Digital Safety Report 2024

A comprehensive analysis of family digital safety practices, emerging online risks, and evidence-based recommendations for protecting children in an increasingly connected world.

RESEARCH REPORT

2024 EDITION

EXECUTIVE SUMMARY

The State of Family Digital Life

94%

Household Connectivity

American families with internet-connected devices in the home

6.2

Average Devices

Connected devices per child under 18 years old

4.5hrs

Daily Screen Time

Average for children ages 8-12, excluding educational use

67%

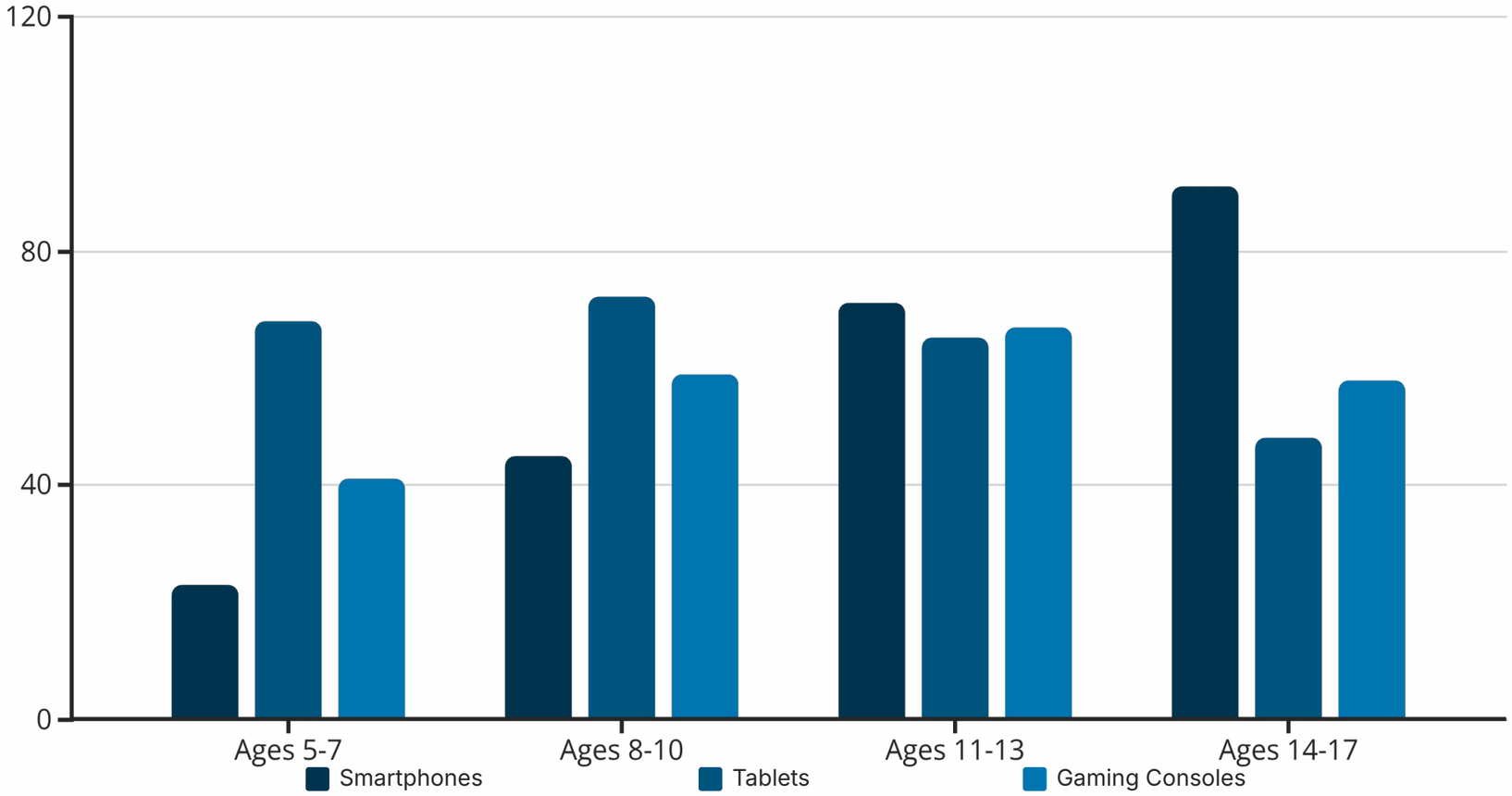
Parental Concern

Parents expressing worry about their child's online safety

CHAPTER 1

Device Usage Patterns Across Age Groups

Our research reveals distinct patterns in how children interact with technology at different developmental stages, with implications for targeted safety strategies.



Smartphone adoption accelerates dramatically in middle school years, while tablet usage peaks in elementary ages and gradually declines as children mature.

CHAPTER 2

Top Online Risks Facing Children Today

Cyberbullying & Harassment

42% of children ages 10-17 report experiencing online harassment, with incidents often originating on social media platforms and gaming communities.

Privacy & Data Exposure

Young users frequently overshare personal information, with 38% posting location data and 56% sharing photos without privacy settings enabled.

Inappropriate Content

Despite safeguards, 61% of teens encounter violent or sexual content unintentionally, primarily through algorithmic recommendations and peer sharing.

Online Predators

Predatory behavior remains persistent, with gaming platforms and social apps being primary contact points. 1 in 9 children receive unwanted sexual solicitations.

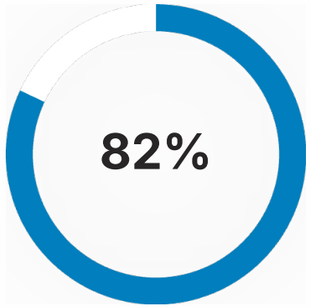
Phishing & Scams

Children lack experience identifying fraudulent schemes. 34% of teens have clicked suspicious links, and 18% have shared passwords with strangers.

The Parental Control Gap

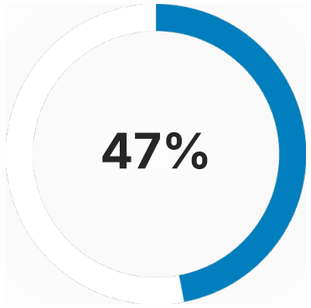
Current Implementation Rates

While awareness of parental controls has increased significantly, actual implementation lags far behind concern levels, creating a substantial protection gap.



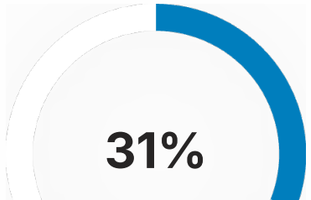
Awareness

Know controls exist



Active Use

Currently enabled



Barriers to Adoption

Technical complexity: 52% find setup too difficult or time-consuming

Multiple devices: Managing controls across platforms is overwhelming

False confidence: 38% believe good communication eliminates need for technical controls

Child resistance: Parents worry about damaging trust or causing conflict

RESEARCH FINDINGS

Effectiveness of Control Strategies

Families employing multiple layers of protection report significantly fewer incidents and greater confidence in their children's online experiences.

Technical Controls

68% reduction in exposure to inappropriate content when filtering and monitoring tools are properly configured and maintained.

Open Communication

73% more likely to report problems when families maintain regular, non-judgmental dialogue about online experiences.

Time Limits

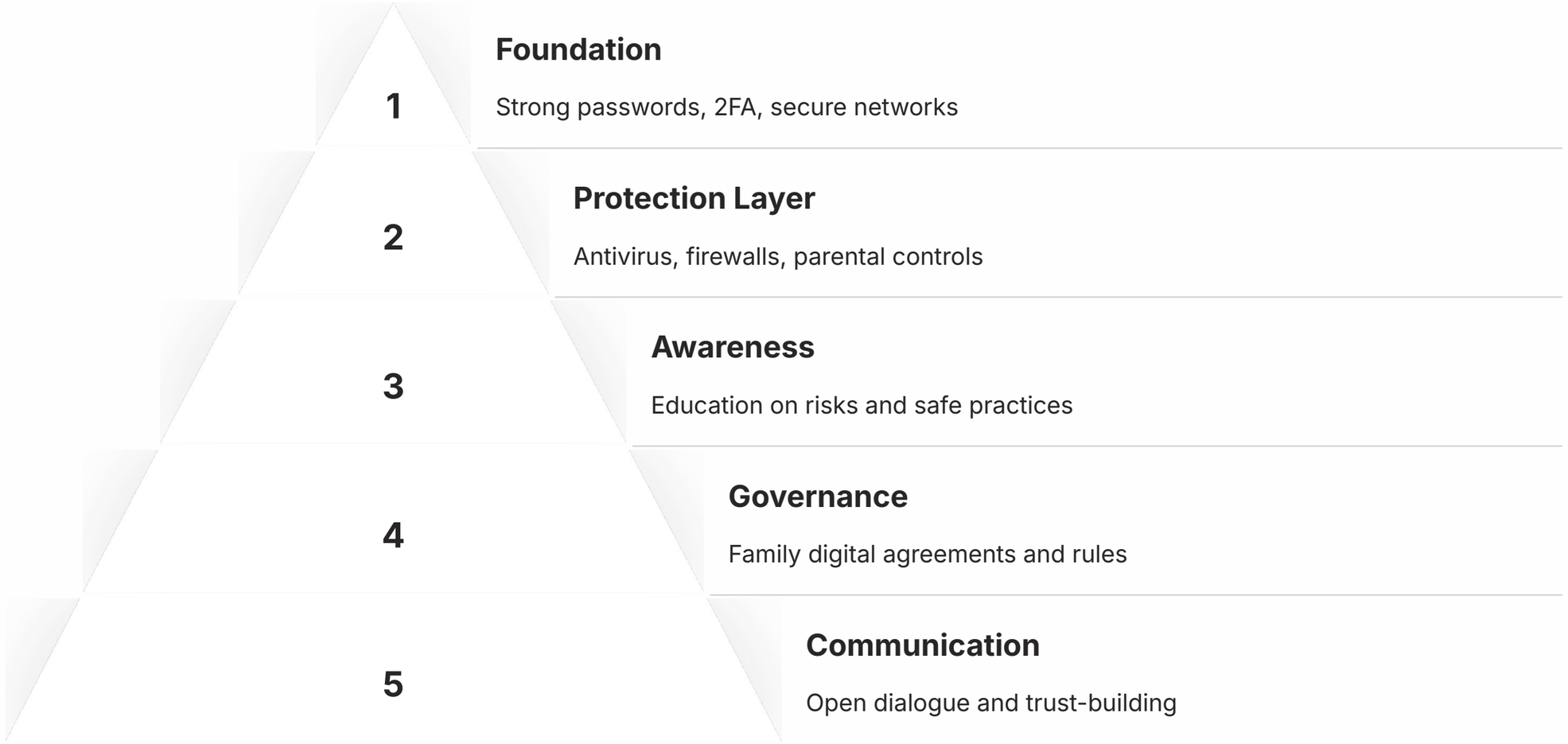
55% improvement in sleep quality and academic performance when screen time boundaries are consistently enforced.

Shared Experiences

4x more effective learning when parents actively participate in children's digital activities rather than just supervising.

CHAPTER 3

Building a Family Cybersecurity Framework



A comprehensive approach combines technical safeguards with education and family culture. Each layer reinforces the others, creating resilient protection that adapts as children grow and technology evolves.

Best Practices: Essential Security Measures

01

Secure Your Home Network

Change default router passwords, enable WPA3 encryption, create a separate guest network for IoT devices, and regularly update firmware.

02

Implement Device Management

Install parental control software on all devices, enable built-in OS protections, and maintain an inventory of connected devices and their security status.

03

Establish Clear Guidelines

Create a family digital agreement covering screen time, acceptable apps, privacy practices, and consequences. Review and update quarterly.

04

Educate Continuously

Hold regular family discussions about online safety, review privacy settings together, and practice identifying scams and suspicious content.

05

Model Good Behavior

Parents must demonstrate the digital habits they expect from children, including limited screen time, strong security practices, and mindful sharing.

06

Monitor & Adapt

Regularly review activity logs, adjust controls as children mature, and stay informed about emerging platforms and risks relevant to your family.

RECOMMENDATIONS

Age-Appropriate Safety Strategies

Elementary (Ages 5-10)

- **Strict supervision**

  Keep devices in common areas, approve all apps before download

- **Limited access**

  Use kid-friendly devices and browsers with strong content filtering

- **Basic education**

  Teach never to share personal information or talk to strangers

Middle School (Ages 11-13)

- **Graduated independence**

  Introduce social media with monitoring, discuss digital reputation

- **Active monitoring**

  Review activity regularly, maintain password access to all accounts

- **Critical thinking**

  Practice identifying misinformation, scams, and manipulative content

High School (Ages 14-17)

- **Trust with verification**

  Reduce direct monitoring while maintaining open communication channels

- **Privacy education**

  Discuss data collection, digital footprints, and long-term consequences

- **Responsibility**

  Involve teens in family security decisions, prepare for independent adulthood

Creating Your Family Digital Agreement

A written agreement establishes clear expectations and provides a framework for consistent enforcement. Involve all family members in the creation process to increase buy-in and compliance.

1

Screen Time Limits

- Daily/weekly maximums by age
- Device-free times and zones
- Educational vs. recreational balance

2

Privacy Standards

- What information can be shared
- Photo and video posting rules
- Location sharing policies

3

Platform Boundaries

- Approved apps and websites
- Age-appropriate content
- Gaming and social media limits

4

Communication Rules

- Who children can contact
- Response to strangers
- Reporting uncomfortable interactions

5

Consequences

- Graduated responses to violations
- Loss of privileges structure
- Path to restoring access

KEY TAKEAWAYS

Essential Actions for Family Digital Safety

Layer Your Defenses

No single solution provides complete protection. Combine technical controls, education, and communication for comprehensive safety.

Adapt as Children Grow

Safety strategies must evolve with developmental stages. What works for a 7-year-old won't work for a 15-year-old.

Prioritize Communication

Children who feel comfortable discussing online experiences with parents are far more likely to report problems and seek guidance.

Stay Current

Digital threats evolve rapidly. Regular education and awareness of new platforms and risks are essential for maintaining protection.

> "The goal isn't to eliminate all risk, but to give children the knowledge, tools, and support they need to navigate the digital world safely and responsibly."

Cyber Security Non-Profit

Making cybersecurity knowledge accessible to everyone

Through education, community, and practical resources, CSNP empowers individuals and organizations to protect themselves in an increasingly digital world. All of our programs and resources are completely free.

Our Programs

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

Learn more about our mission and programs

Access free cybersecurity resources