Be Sure & Secure

Empowering Families to Protect What Matters Most

Teach Them Diligently • May 9, 2026

Sean Ardizzone | CEO, ArkCybr | OSCP, CEH, Security+

B · E · S · U · R · E

ABOUT

Who Is Sean Ardizzone?

Certifications & Background

- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- Certified Cybersecurity Analyst (E|CSA)
- Certified Ethical Hacker (C|EH)
- CompTIA Security+ CE
- ITIL v3 Foundation
- 30+ years public & private sector security
- US Army Combat Veteran, OIF 2004–2005

Who I Am

- Christian, Husband, Father of 4
- CEO & Founder — ArkCybr
- New homeschool dad to AJ*

Why I Do This

I founded ArkCybr in 2021 after the passing of my son, Alex — who wanted to be a hacker just like his dad.

I was exposed to harmful content at age 11 — long before most families had any tools to prevent it. That experience shaped everything.

My mission: give every family access to the same cybersecurity expertise that corporations pay millions for — for free or close to it.

"Beauty from ashes." — Isaiah 61:3

What We're Covering Today

01	Welcome & Why This Matters	5 min
02	The Threat Landscape Families Face	7 min
03	Introducing the BE SURE Framework	5 min
04	B — Backups	
05	E — Encryption	
06	S — Secure Your Devices	
07	U — Update Regularly	35 min total
08	R — Reduce Harmful Content	
09	E — Educate Your Family	
10	Q&A, Checklist & Action Steps	5 min

THREAT LANDSCAPE

The Digital World Your Family Lives In

1 in 3

children encounter harmful content online before age 13

$6.9T

global cybercrime costs projected for 2025

95%

of cyberattacks are caused by human error — not tech failure

83%

of teens report being contacted by strangers online

Threats Your Family Faces Every Day

Phishing

Fake emails, texts, and sites designed to steal passwords or install malware. Kids are primary targets.

Ransomware

Malicious software that locks your files and demands payment. Families lose irreplaceable photos, school work, and finances.

Predatory Apps

Platforms with hidden chat features that expose children to grooming and exploitation by bad actors.

Harmful Content

Pornography, violent content, and radicalization pipelines — often served algorithmically without warning.

Social Engineering

Manipulating people — including children — into giving up access, money, or private information.

Weak Credentials

Reused or simple passwords are the #1 entry point for attackers across all devices in your home.

THE FRAMEWORK

The BE SURE Framework

A faith-rooted, practical system for protecting your family in the digital age

B	E	S	U	R	E
Backups	**Encryption**	**Security**	**Update**	**Reduce Risk**	**Educate**
Preserve what God has entrusted	Guard private info as a family value	Lock down devices and accounts	Renew and transform your defenses	Cut off harmful content at the source	Equip your family with wisdom

"Sanctify them by Your truth. Your word is truth."
— John 17:17

Backups — Guard What Was Entrusted

Stewardship is a biblical principle. Your family photos, school records, financial documents, and memories are irreplaceable. A single ransomware attack or hard drive failure can erase years of digital life.

> *"As each has received a gift, use it to serve one another, as good stewards of God's varied grace."*
> **— 1 Peter 4:10**

B

3-2-1 Backup Rule

- 3 copies of your data
- 2 different storage types (e.g. drive + cloud)
- 1 stored offsite or in the cloud

Free Tools for Families

- Google Drive / OneDrive (15–20GB free)
- BackBlaze Personal ($9/mo)
- External hard drive rotated monthly

What to Back Up

- Family photos & videos
- School work and documents
- Financial records and tax files
- Device backups (iCloud, Samsung Cloud)

Encryption — Securing Privacy as a Family Value

"Come out from among them and be separate," says the Lord. — 2 Corinthians 6:17

Encryption = a digital lock on your information. Without it, your emails, messages, and files can be read in transit by anyone on the same network.

E

Device Encryption

- iPhone — enabled by default with passcode
- Android — Settings → Security → Encryption
- Windows — BitLocker (Pro) or Device Encryption
- Mac — FileVault (System Preferences → Security)

Communication Encryption

- Use Signal or iMessage for private family chats
- Avoid SMS for sensitive info — it's not encrypted
- Email: ProtonMail for sensitive messages
- Never send passwords over regular email or text

Home Network Security

- Set Wi-Fi to WPA3 or WPA2 (check router settings)
- Change default router password immediately
- Create a separate guest network for visitors
- Avoid hotel/café Wi-Fi for banking or accounts

Security — Lock Down Every Device & Account

"But whoever listens to me will dwell in safety, secure from the fear of evil.”" **— Proverbs 1:33**

S

Passwords & Accounts

- 15+ char: upper, lower, numbers, symbols
- Never reuse passwords across accounts
- Use a password manager: Bitwarden (free), 1Password
- Enable 2FA/MFA on every account that allows it
- Authenticator app preferred over SMS

Device Lockdown

- Require PIN/password to unlock
- Review and revoke unused app permissions regularly
- Disable 'open Wi-Fi auto-connect' on phones
- Use “least privilege” accounts

Home Network

- Change default router login (admin/admin is unsafe)
- Use WPA2/WPA3 encryption on your Wi-Fi
- Segment: family vs. guest vs. IoT devices
- Disable WPS (easy to crack)
- Review connected devices list regularly

Update — Transformation, Not Conformity

“Be very careful, then, how you live—not as unwise but as wise, making the most of every opportunity, because the days are evil." — Ephesians 5:15-16

Most successful cyberattacks exploit vulnerabilities that had patches available weeks or months before the attack. Keeping software current is the single highest-ROI security action a family can take.

U

Why 'I'll Do It Later' Is Dangerous

- Attackers scan for unpatched devices within hours of a public CVE
- Turn on automatic updates for Windows, macOS, iOS, and Android
- Router firmware must be checked manually (check manufacturer site quarterly)
- Smart TVs, tablets, gaming consoles — these need updates too
- Unsupported devices (Windows 7, old phones) = active network risk

Building the Update Habit

- Set a monthly 'family tech review' reminder in your calendar
- After a major OS update — restart fully and verify it completed
- Check all app stores weekly for pending app updates
- Subscribe to CISA alerts — free, plain-English summaries
- Teach kids: 'Update now' is a required security action, not optional

Reduce Risk — Remove Access to Harmful Content

R

"Do not set foot on the path of the wicked... Avoid it; do not travel on it." **— Proverbs 4:14-15**

DNS-Level Content Filtering

DNS filtering stops harmful sites before they ever load — at the network level, across every device in your home.

ArkCybr: blocks malicious domains, adult content, and known threat sources.

Free: CleanBrowsing, OpenDNS FamilyShield, Quad9
Managed: NextDNS, Cisco Umbrella

Device-Level Controls

iOS: Screen Time → Content & Privacy Restrictions

Android: Google Family Link — monitor and restrict from parent device

Paid apps: Bark, Circle, Covenant Eyes — monitoring and accountability

YouTube: YouTube Kids app or Restricted Mode enabled

Filters are tools, not parenting. Combine technology with open, faith-centered conversations about what your family values — and why the digital world requires both wisdom and guardrails.

Educate Yourself & Others — Walk in Truth, Expose the Darkness

"Take no part in the unfruitful works of darkness, but instead expose them." — Ephesians 5:11

E

Age-Appropriate Conversations

- Ages 5–8: 'Strangers online are still strangers'
- Ages 9–12: Privacy, screenshots, online permanence
- Ages 13+: Identity, predatory tactics, sexting laws
- All ages: You can always come to me without punishment

Teaching Digital Discernment

- If it makes you feel bad, tell a trusted adult
- Not everything you read online is true
- Your online actions have real-world consequences
- Faith lens: Would Jesus scroll past this?

Family Agreements & Habits

- Create a Family Technology Agreement together
- Devices charge outside bedrooms at night
- No screens at meals — undivided presence
- Regular family 'digital check-in' conversation

Resources to Use Together

- Common Sense Media — age ratings for apps & games
- ArkCybr SafetyNet Podcast — family cybersecurity
- CISA Kids/Teens Safety Resources (free)
- Make digital safety part of your family Bible study

Your 30-Day Family Security Action Plan

Week 1

- ✓ Set up 3-2-1 backup for all family devices
- ✓ Enable encryption on phones & computers
- ✓ Change your router's default password

Week 2

- ✓ Install a password manager for the family
- ✓ Enable 2FA on email, banking & social media
- ✓ Review and update all app permissions

Week 3

- ✓ Set up DNS-level content filtering on router
- ✓ Enable parental controls on kids' devices
- ✓ Review connected devices on home network

Week 4

- ✓ Hold your first family 'Tech Talk' meeting
- ✓ Create your Family Technology Agreement
- ✓ Schedule monthly 'digital check-in' reminders

Download the full BE SURE Family Checklist at arkcybr.com

FOUNDATION

We Are Called to Digital Stewardship

1 Peter 4:10

"As each has received a gift, use it to serve one another, as good stewards of God's varied grace."

Proverbs 4:14-15

"Do not set foot on the path of the wicked or walk in the way of evildoers. Avoid it; do not travel on it."

Romans 12:2

"Do not be conformed to this world, but be transformed by the renewal of your mind, that by testing you may discern what is the will of God."

John 17:17

"Sanctify them by Your truth. Your word is truth. I have given them Your word and the world has hated them because they are not of the world."

Let's Do It Together — Live Demonstration

Pull out your phone. We'll walk through 3 quick security wins right now.

1 Check Your Screen Lock

Estimated time: 2 min

Settings → Face/Touch ID & Passcode

Verify auto-lock is set to 30 sec – 1 min

Upgrade 4-digit PIN to 6-digit or alphanumeric

2 Enable 2FA on Your Email

Estimated time: 3 min

Gmail: Account → Security → 2-Step Verification

Outlook: Account Security → Advanced Security

Choose authenticator app over SMS when possible

3 Review App Permissions

Estimated time: 3 min

iOS: Settings → Privacy & Security → Location

Android: Settings → Privacy → Permission Manager

Revoke location/mic/camera from untrusted apps

COMMON MISTAKES

5 Mistakes That Leave Your Family Exposed

01	**Shared family passwords**	→ Every person, every account gets a unique password. Use a family password manager to make it easy.
02	**Kids have unsupervised devices in bedrooms**	→ Devices charge in common areas. No screens after a set time. Conversation over surveillance.
03	**Trusting 'free' VPNs or security tools**	→ Free VPNs often sell your data. Use reputable paid options — or consult a trusted expert first.
04	**No family incident response plan**	→ Decide now: who do you call if your account is hacked? What's the first step? Write it down.
05	**Assuming kids know this stuff already**	→ Digital natives are not digitally safe. Tech fluency and security awareness are very different skills.

Questions?

Let's work through your specific questions together.

Website	Free Family Resources	Podcast
arkcybr.com	**arkcybr.com/convention**	**SafetyNet by ArkCybr**

Be Sure. Be Secure.

Be Faithful.

Your family is worth protecting. You have everything you need to start today.

---

① Start your backup this week

② Enable 2FA on one account today

③ Have the talk with your kids tonight

arkcybr.com | Free family security resources & the BE SURE checklist