Why the Family Cyber Safety Framework (FCSF v1.0)?

The internet has become the family's new playground, classroom, bank, and social space. Children stream, play, learn, and socialize online. Parents pay bills, store memories, and manage their lives in digital form. Yet every one of these activities opens a door to cyber threats - phishing scams, identity theft, predators, and ransomware - dangers once reserved for companies but now reaching directly into our homes.

Professional cybersecurity frameworks like NIST, ISO, or the CIS Controls have shown businesses how to protect themselves. But they're written in technical language, assuming budgets, IT teams, and professional expertise. Ordinary families - the people who arguably have the most at stake - are left with scattered tips, confusing settings, and no single, trusted roadmap to follow.

The Family Cyber Safety Framework (FCSF) was created to close that gap. It takes the world's most trusted cybersecurity principles and reshapes them into plain language and simple activities. Instead of a complex framework and hundreds of controls, it offers **3 steps** and **16 practical activities** a nontechnical parent can implement in hours, not months.

By adopting FCSF, families gain:

- **Clarity** - a one-page set of house rules everyone can understand.
- **Protection** - strong, automatic defenses like secure Wi-Fi, backups, and parental control.
- **Preparedness** - a short plan for what to do when a device is lost or an account is hacked.
- **Resilience** - the ability to recover memories, finances, and peace of mind after an incident.

In short, the Family Cyber Safety Framework brings the rigor of professional cybersecurity into the everyday household, bridging the gap between expert knowledge and real-world family life. It empowers parents, protects children, and builds digital safety skills - without requiring any previous technical expertise.

www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454

The Framework

The FCSF is built of three easy to remember **Steps**:

1. **Prepare -** set the house rules and who does what, list the people, devices, and accounts to protect.
2. **Protect -** put the everyday protection in place, notice when something's wrong.
3. **Respond -** follow a short plan when trouble happens, restore your stuff and improve for next time.

These three steps create a clear path to security: **Prepare** sets direction, and makes assets visible, **Protect** prevents problems and detects early, **Respond** limits damage, restores and improves.

The framework includes **16 Activities** to be performed to achieve these steps. Together, they form an easy-to-teach, repeatable framework that grows with your family.

www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454

Prepare

This is the "family constitution" of your digital life. It's about deciding what you care about, who's responsible for what, and how decisions get made. In this step you create a "map" of the digital home. You can't protect what you don't know exists.

Purpose:

- Establish clear house rules so everyone knows boundaries and expectations.
- Define who is the "admin" and who can make changes to settings or buy new devices.
- List the people, devices, and accounts (assets) you need to protect.
- Spot which assets are "critical" (email, bank, school portal).
- Track devices and accounts as changes are made.

Importance:

Without this, the family's security is ad-hoc. Setting simple written rules dramatically reduces mistakes. It also empowers children because they understand what's allowed and why. Families often forget an old tablet or an unused account, which can be hijacked. By simply listing assets, you make the invisible visible and reduce blind spots.

Activities:

1) **Define Family Cyber Rules** – One page of house rules: time online for children, what's private, define Roles and Permissions, who uses admin and who uses standard accounts.
   Review Frequency: Review once a year
2) **Create Devices and Accounts list** – the list includes **Devices that need protection** (phones, tablets, PCs, smart TV, router, cameras, game consoles), **Account Inventory** (emails, banking, socials, gaming, school portals) classified according to their criticality and **who uses what** (parents, kids, grandparents, visitors).
   Review Frequency: Review once a year or when a change happens

Examples in Practice:

- One-page "Family Cyber Rules."
- Parents make purchases, set router passwords, and app approvals.
- Device & Account Inventory Sheet.
- Marking accounts as "critical" for priority security.

Protect

This step is about **everyday shields** - putting locks on digital doors and windows and **noticing problems quickly**.

Purpose:

- Create strong barriers to unauthorized access.
- Limit damage if one account or device is compromised.
- Keep private data private.
- Spot suspicious activity early before it causes major harm.
- Give you time to react, lock down accounts, and protect finances or privacy.

Importance:

Most attacks succeed because of weak passwords, outdated software, or open networks. Simple protective habits cut 80%+ of common risks. Families rarely "monitor" their digital life, but early detection often makes the difference between a minor inconvenience and a major problem.

Activities:

3) **Set Strong Sign-in** – password manager + unique passphrases + 2-step login on critical accounts (email/bank/social).
   Review Frequency: Every six months
4) **Protect Devices** - Antivirus on Computers, App hardening and permissions review on Smartphones, SW based Firewall.
   Review Frequency: Every six months
5) **Ensure Safe Browsing** – Subscribe to the DNS family filter.
   Review Frequency: Every six months
6) **Update Everything** – auto-updates on OS, apps, router/IoT firmware.
   Review Frequency: Every six months
7) **Define Safe Network** – WPA2/3, new router admin password, router auto-updates or scheduled firmware checks, guest/IoT network separation from home NW.
   Review Frequency: Every six months
8) **Activate Parental Control** – age filters, app store approval, screen-time limits.
   Review Frequency: Every six months
9) **Ensure Privacy by Default** – private profiles, location sharing off by default, minimal data in forms.

Review Frequency: Every six months

10) **Create Backups** – 3 copies, 2 types of media, 1 on cloud.
    Review Frequency: Every six months
11) **Activate Security Alerts** – email/login alerts on major accounts; bank/SMS alerts for transactions.
    Review Frequency: Every six months
12) **Perform Home Check-ups** – monthly 10-minute review: new devices? updates failed? odd emails? Backup failed? Etc.
    Review Frequency: Monthly

Examples in Practice:

- Strong, unique passwords managed by a password manager.
- Auto-updates on all devices, including the router.
- Separate guest/IoT network plus DNS filtering for family-friendly browsing.
- Backups (3-2-1 rule) for photos and documents.
- Email or SMS alerts for new logins or bank transactions.
- Quick monthly check-ups for odd emails or failed updates.

Respond

This is your **emergency drill**, helps you to understand if you are ready for incident, to **respond** if something happens, **bouncing back** quickly and **learn** from incidents.

Purpose:

- Have a simple plan so panic doesn't set in.
- Ensure everybody knows what to do if something happens.
- Minimize damage and recover faster. Get back to normal quickly after an incident.
- Learn lessons to prevent repeats.

Importance:

Most people freeze or make poor decisions during digital crises. Practicing in advance, even just once, empowers the whole household. Without recovery, a ransomware infection or lost device can erase priceless family memories or disrupt school/bank access. Recovery ensures resilience.

Activities:

13) **Define "What If" plan** – Create a list of "what If" scenarios, simple list that will be used as incident response plan (e.g., disconnect Wi-Fi, change password, call bank/school). The What If plan helps us to adopt the "stop-think-act" approach.
    Review Frequency: Yearly
14) **Lost Device Playbook** – What actions to take if a device is lost (locate/lock/wipe with Find My/Android Device Manager, change major passwords).
    Review Frequency: Yearly
15) **Restore & Reset Procedure** – How to clean reinstall if malware suspected, restore from backup, re-enable 2-step login.
    Review Frequency: Yearly
16) **Learn & Improve** – Write 2 lines: what happened, what to change (e.g., add 2FA for X, move camera to guest Wi-Fi).
    Review Frequency: When incident happens

Examples in Practice:

- “Stop–Think–Act” mini-incident plan: disconnect Wi-Fi, change passwords, enable account recovery.
- Lost Device Playbook: locate, lock, wipe, change major passwords.
- Prepared contact info for banks, schools, or local authorities.
- Regular backups stored in cloud.
- Wiping and reinstalling a device, then restoring from backup.
- Reviewing what happened and updating house rules or security settings.

www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454

Framework Implementation

You do not have to perform all 16 Activities at once. There are 3 implementation levels so that you can Start Small and Grow Naturally.

Level A (Basic Hygiene) - Start with creating Device & Accounts list (2) and activities 3, 4, 5, 6, 10.

Level B (Family Ready) - Add activities 1, 8, 9, 11 and 14.

Level C (Resilient Home) - Add activities 7, 12, 13, and perform a drill with lessons learned (15, 16).

"10-Minute Monthly" Checklist

☐ Updates succeeded on phones/PC/router

☐ Backups ran

☐ Password manager health: no reused/weak passwords

☐ Bank/login alerts reviewed

☐ New device? put it on guest/IoT Wi-Fi

☐ Kids' apps & privacy settings spot-check

Simple Metrics to see your progress:

- **% Critical accounts with 2-step login** (target: 100%)
- **Backup recency** (days since last successful backup; target: ≤7)
- **Weak/reused passwords count** in the manager (target: 0)
- **Time to lock a lost phone** during a drill (target: <10 minutes)

www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454

Summary

The Family Cyber Safety Framework (FCSF) is an easy-to-follow framework designed specifically for households and families. It adapts proven principles from NIST CSF, ISO/IEC 27001, and the CIS Critical Security Controls to help non-technical parents and guardians protect their homes, children, and personal data.

Step	Activity	Description	Review Frequency
Prepare	(1) Family Cyber Rules	One page of house rules: time online for children, what's private, define Roles and Permissions, who uses admin and who uses standard accounts.	Yearly
	(2) Devices and Accounts list	The list includes Devices that need protection (phones, tablets, PCs, smart TV, router, cameras, game consoles), Account Inventory (emails, banking, socials, gaming, school portals) classified according to their criticality and who uses what (parents, kids, grandparents, visitors).	Yearly or when a change happens
Protect	(3) Strong Sign-in	Password manager + unique passphrases + 2-step login on critical accounts (email/bank/social).	Every six months or when new account is added
	(4) Safe Devices	Antivirus on all Computers and Smartphones, SW based Firewall.	Every six months or when new Device is added
	(5) Safe Browsing	DNS family filter.	Every six months or when new device is added
	(6) Update Everything	Auto-updates on OS, apps, router/IoT firmware.	Every six months or when new

www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454

			device is added
	(7) Safe Network	WPA2/3, new router admin password, guest/IoT network, DNS family filter.	Every six months or when new device is added
	(8) Parental Control	Age filters, app store approval, screen-time limits.	Every six months or when new device is added
	(9) Privacy by Default	Private profiles, location sharing off by default, minimal data in forms.	Every six months
	(10) Backups	3 copies, 2 types of media, 1 on cloud.	Every six months
	(11) Security Alerts	Email/login alerts on major accounts; bank/SMS alerts for transactions.	Every six months
	(12) Home Check-ups	Monthly 10-minute review: new devices? updates failed? odd emails?	Monthly
Respond	(13) "What If" plan	Create a list of "what If" scenarios, simple list that will be used as incident response plan (e.g., disconnect Wi-Fi, change password, call bank/school). The What If plan helps us to adopt the "stop-think-act" approach.	Yearly
	(14) Lost Device Playbook	What actions to take if a device is lost (locate/lock/wipe with Find My/Android Device Manager, change major passwords). Review Frequency: Yearly	Yearly
	(15) Restore & reset	How to clean reinstall if malware suspected, restore from backup, re-enable 2-step login.	Yearly + Yearly Drill
	(16) Learn & improve	Write 2 lines: what happened, what to change (e.g., add 2FA for X, move camera to guest Wi-Fi).	When incident happens

The Family Cyber Safety Framework is a fresh, practical approach for households. By following its Steps families can dramatically reduce risk, protect personal data, and teach children digital life skills.

www.aidit.co.il | roman.vaintraub@aidit.co.il | +972 54 2482454