TOOLKIT GUIDE
English

ZERODAY TECH LABS

Household Cyber Safety Toolkit

A complete English guide with practical checklists for the home.

Audience	Families, older adults, children, caregivers, and community helpers.
Purpose	Bring the main household safety guides into one complete document.
Best use	Use as the main printed Toolkit for workshops and family reference.

Start with these actions

[ ]	Protect email first because it resets many other accounts.
[ ]	Use a long unique password for email, banking, and phone carrier accounts.
[ ]	Turn on multifactor authentication for email, banking, social media, and cloud accounts.
[ ]	Turn on automatic updates for phones, computers, browsers, and apps.
[ ]	Do not click links in surprise bank, package, prize, or support messages.
[ ]	Ask a trusted person before sending money, codes, passwords, or gift cards.

Family rule

If a message creates fear, pressure, or secrecy, pause before acting. Real support should allow calm verification.

Next step

Open the baseline checklist and the stop verify report playbook. They turn this quick start into a repeatable home routine.

Router and Wi Fi

[ ]	Change the router admin password.

[ ]	Use WPA3 or WPA2 WPA3 if available.
[ ]	Turn off WPS if the household does not use it.
[ ]	Turn off remote admin access unless it is truly needed.
[ ]	Create guest Wi Fi for visitors and smart devices when possible.

Accounts and devices

[ ]	Protect email with multifactor authentication.
[ ]	Use different passwords for important accounts.
[ ]	Turn on updates for phones, computers, browsers, and apps.
[ ]	Remove unused apps and browser extensions.
[ ]	Back up important photos and documents.

Review schedule

Do a short review every three months. Check updates, passwords, backups, and unknown devices.

Stop

[ ]	Do not click links.
[ ]	Do not open attachments.
[ ]	Do not reply to the sender.
[ ]	Do not share passwords, codes, or payment details.
[ ]	Take a screenshot if it is safe.

Verify

[ ]	Use the official website or app you already know.
[ ]	Call a trusted number from a card, statement, or official website.
[ ]	Ask a trusted family member or helper.
[ ]	Check whether the message creates fear or urgency.

Report

[ ]	Forward scam texts to 7726 when available.
[ ]	Report fraud at ReportFraud.ftc.gov.
[ ]	Report internet crime at IC3.gov when appropriate.
[ ]	Report identity theft at IdentityTheft.gov.

Do this first

[ ]	Disconnect the suspicious device from the internet if needed.
[ ]	Do not enter new passwords on a device that may be compromised.
[ ]	From a clean device, change the email password first.
[ ]	Enable multifactor authentication.
[ ]	Check recent logins and sign out of unknown sessions.
[ ]	Call the bank or card issuer if money or payment data may be involved.

Clean and recover

[ ]	Run a built in security scan.
[ ]	Apply updates.
[ ]	Remove suspicious apps or browser extensions.
[ ]	Restore files from backup if needed.
[ ]	Save screenshots and notes for reporting.

Do not do this

[ ]	Do not share codes with a caller.
[ ]	Do not allow remote access because a pop up told you to.
[ ]	Do not pay a stranger who claims they can remove a virus.

Children

[ ]	Ask a trusted adult before clicking links or downloading games.
[ ]	Do not share real name, address, school, photos, or passwords online.

[ ]	If a message feels scary or urgent, show an adult.

Teens

[ ]	Use multifactor authentication on email, school, gaming, and social accounts.
[ ]	Do not reuse passwords.
[ ]	Do not send private photos to strangers.
[ ]	Check privacy settings and location sharing.

Adults

[ ]	Protect email first.
[ ]	Use unique passwords and a password manager.
[ ]	Treat delivery, banking, job, and tech support messages as suspicious until verified.
[ ]	Back up important files.

Older adults

[ ]	Do not trust surprise calls about viruses, refunds, locked accounts, gift cards, or emergencies.
[ ]	Hang up and call back using a trusted number.
[ ]	Do not let a caller control your computer.
[ ]	Ask a trusted person before sending money or codes.

Keep this guide near the device or account it protects. Small habits make a real difference when they are repeated.