



Household Cyber Safety Toolkit

Kit de Seguridad Cibernética para el Hogar

Printable checklists, quick start guides, and step by step exercises (EN/ES).

Checklists, guías rápidas y ejercicios paso a paso (EN/ES).

Prepared by Joseph R. González Ríos • Polytechnic University of Puerto Rico

Version Version 1.0 • January 2026

Use Educational use • No logins • No sensitive data collection

Safety promise: This toolkit will never ask for passwords, MFA codes, or logins. If anyone asks, treat it as a scam.

Quick Start

Inicio rapido

English

- Start with the Baseline Checklist. Secure the router admin password, Wi-Fi encryption, and auto updates.
- Protect your email first: enable MFA and use a long, unique passphrase.
- Use the Stop Verify Report script for unexpected messages (email, texts, calls).
- Set up backups and test restoring one file so recovery is possible if something goes wrong.

Espanol

- Empieza con la Lista Basica. Asegura el password admin del router, cifrado Wi-Fi y auto updates.
- Protege el email primero: activa MFA y usa una frase larga y unica.
- Usa Detente Verifica Reporta para mensajes inesperados (email, textos, llamadas).
- Configura backups y prueba restaurar un archivo para poder recuperarte si pasa algo.

Contents / Contenido

Minimum Home Network Baseline Checklist / Lista Basica Minima del Hogar	3
30 Day Home Improvement Plan / Plan de 30 Dias	7
Stop Verify Report Playbook / Guia Detente Verifica Reporta	9
Incident Response & Recovery Checklist / Lista de Respuesta y Recuperacion	11
Age-Tailored Cyber Safety Cards / Tarjetas de Ciberseguridad por Edad	13

Note: Print only the pages you need. Links point to official resources.

Minimum Home Network Baseline Checklist

A fast, low-cost security baseline for most households (15-30 min to start).

Checklist

Router & Wi-Fi

- ☐ Change the router ADMIN password (not the Wi-Fi password).
- ☐ Update router firmware (enable auto update if available).
- ☐ Use WPA3 (or WPA2/WPA3). Avoid WEP.
- ☐ Turn off WPS (Wi-Fi Protected Setup) if you do not use it.
- ☐ Use Guest Wi-Fi for visitors and (if possible) a separate network for IoT devices.
- ☐ Disable remote admin access and UPnP if you do not need them.

Accounts & MFA

- ☐ Enable MFA on email first, then bank, then social media.
- ☐ Use a password manager (or written plan) to avoid password reuse.
- ☐ Use long, unique passphrases for key accounts.
- ☐ Store recovery codes in a safe place (not only on the same phone).

Devices & Updates

- ☐ Turn on automatic updates on phones, computers, browsers, and key apps.
- ☐ Remove apps/extensions you do not use.
- ☐ Use built-in security tools (e.g., Windows Security) and keep them updated.

Backups & Recovery

- ☐ Set up at least one backup method (cloud and/or external drive).
- ☐ Disconnect external backup drives when not backing up.
- ☐ Test restoring one file (proof your backup works).

Household habits

- ☐ Use Stop / Verify / Report for unexpected messages.
- ☐ Download apps only from official stores.
- ☐ Talk as a family about scams and what to do if something feels 'off'.

Quick Readiness Score (optional)

- ☐ Email has MFA
- ☐ Router admin password changed
- ☐ Auto-updates enabled on main devices
- ☐ Backups configured

[] Guest Wi-Fi enabled

[] No password reuse (or actively being fixed)

Count how many you have (0-6). Use it to prioritize what to fix next - not to judge.

Safety note: This checklist avoids risky steps. If changing router settings breaks Wi-Fi, you can revert or contact your ISP using official support channels.

Official resources

[NSA: Best Practices for Securing Your Home Network \(PDF\)](#)

[CISA: Secure Our World](#)

[CISA: Secure Our World Tip Sheets \(Spanish\)](#)

Checklist Baseline Mínimo de Seguridad en el Hogar

Un baseline rápido y de bajo costo para la mayoría de hogares (15-30 min para empezar).

Checklist

Router & Wi-Fi

- ☐ Cambia la contraseña ADMIN del router (no la del Wi-Fi).
- ☐ Actualiza firmware del router (auto update si existe).
- ☐ Usa WPA3 (o WPA2/WPA3). Evita WEP.
- ☐ Apaga WPS si no lo usas.
- ☐ Usa red de invitados para visitas y (si puedes) una red separada para IoT.
- ☐ Desactiva admin remota y UPnP si no lo necesitas.

Cuentas & MFA

- ☐ Activa MFA en email primero, luego banca, luego redes sociales.
- ☐ Usa gestor de contraseñas (o plan escrito) para evitar reutilizar.
- ☐ Usa frases largas y únicas para cuentas clave.
- ☐ Guarda códigos de recuperación en lugar seguro (no solo en el celular).

Dispositivos & Updates

- ☐ Activa actualizaciones automáticas en teléfonos, computadoras, navegador y apps.
- ☐ Elimina apps/extensiones que no uses.
- ☐ Usa herramientas de seguridad integradas y mantenlas al día.

Backups & Recuperación

- ☐ Configura al menos un método de backup (nube y/o disco externo).
- ☐ Desconecta el disco externo cuando no esté haciendo backup.
- ☐ Prueba restaurar un archivo (confirmar que funciona).

Hábitos del hogar

- ☐ Usa Detente / Verifica / Reporta con mensajes inesperados.
- ☐ Descarga apps solo de tiendas oficiales.
- ☐ Habla en familia sobre estafas y qué hacer si algo se siente raro.

Puntaje rápido de preparación (opcional)

- ☐ Email tiene MFA
- ☐ Password admin del router cambiado
- ☐ Auto-updates activos en dispositivos principales

- [] Backups configurados
- [] Red de invitados activa
- [] No reutilizas contraseñas (o lo estás arreglando)

Cuenta cuántas tienes (0-6). Sirve para priorizar, no para juzgar.

Nota de seguridad: Este checklist evita pasos riesgosos. Si un cambio rompe el Wi-Fi, puedes revertir o contactar tu ISP por canales oficiales.

Recursos oficiales

[NSA: Best Practices for Securing Your Home Network \(PDF\)](#)

[CISA: Secure Our World](#)

[CISA: Secure Our World Tip Sheets \(Spanish\)](#)

30 Day Home Cyber Improvement Plan

Small steps, big impact. Aim for 15-20 minutes per session.

Week 1: Protect accounts

- ☐ Enable MFA on email.
- ☐ Install/setup a password manager (or choose a safe method).
- ☐ Change 3 reused passwords (email, bank, social).
- ☐ Save recovery codes in a safe place.

Week 2: Update and clean devices

- ☐ Turn on auto updates (phone + computer).
- ☐ Update browser and remove unused extensions.
- ☐ Run a built-in security scan.
- ☐ Remove unused apps.

Week 3: Secure Wi-Fi and IoT

- ☐ Change router admin password.
- ☐ Set WPA3 or WPA2/WPA3; change Wi-Fi password.
- ☐ Enable Guest Wi-Fi and use it for visitors.
- ☐ Update smart TV/camera/console firmware; move IoT to Guest/IoT network if possible.

Week 4: Backups and recovery

- ☐ Set up backups (cloud and/or external drive).
- ☐ Disconnect external drive when done.
- ☐ Test restore one file.
- ☐ Do a family phishing practice: Stop / Verify / Report.

Finish line

- Write down where you report scams: 7726, ReportFraud.ftc.gov, ic3.gov.
- Pick one day per month to do updates + quick checks.
- Share the plan with another household (it helps to stay consistent).

Official resources

[CISA: Secure Our World](#)

[NSA: Best Practices for Securing Your Home Network \(PDF\)](#)

Plan de 30 Días para Mejorar la Ciberseguridad en Casa

Pasos pequeños, impacto grande. 15-20 minutos por sesión.

Semana 1: Proteger cuentas

- [] Activa MFA en email.
- [] Instala/configura un gestor de contraseñas (o método seguro).
- [] Cambia 3 contraseñas repetidas (email, banca, redes).
- [] Guarda códigos de recuperación en lugar seguro.

Semana 2: Actualizar y limpiar dispositivos

- [] Activa auto updates (teléfono + computadora).
- [] Actualiza navegador y elimina extensiones que no uses.
- [] Corre escaneo de seguridad integrado.
- [] Elimina apps que no uses.

Semana 3: Asegurar Wi-Fi e IoT

- [] Cambia password admin del router.
- [] Activa WPA3 o WPA2/WPA3; cambia password del Wi-Fi.
- [] Activa red de invitados y úsala para visitas.
- [] Actualiza firmware de smart TV/cámara/consola; mueve IoT a red separada si se puede.

Semana 4: Backups y recuperación

- [] Configura backups (nube y/o disco externo).
- [] Desconecta el disco externo al terminar.
- [] Prueba restaurar un archivo.
- [] Haz un ejercicio: Detente / Verifica / Reporta.

Para cerrar

- Anota dónde reportar: 7726, ReporteFraude.ftc.gov, ic3.gov.
- Elige un día al mes para updates + chequeos rápidos.
- Comparte el plan con otro hogar (ayuda a mantener el habito).

Recursos oficiales

CISA: [Secure Our World](#)

NSA: [Best Practices for Securing Your Home Network \(PDF\)](#)

Stop Verify Report Playbook

A simple script for phishing, smishing, and scam calls.

3 steps

STOP

- Do not click links or open attachments.
- Do not reply or argue with the scammer.
- Take a screenshot for evidence.

VERIFY

- Use official channels: type the website yourself or use the official app.
- Call a trusted number (from your card, statement, or official website).
- Ask a trusted person if you feel pressured.

REPORT

- Forward scam texts to SPAM (7726).
- Report scams at ReportFraud.ftc.gov (Spanish: ReporteFraude.ftc.gov).
- Report cyber-enabled crime at ic3.gov.

Quick scripts

Bank message: I received a message about my account. I'm calling the number on my card to verify. Can you confirm if this is real?

Delivery/text link: I'm not clicking links in texts. I'll check tracking in the official app/website.

Tech support pop-up/call: I did not request support. I will close this window and contact the company through its official support site.

Family emergency: I'm going to call you back on your saved number to confirm.

Red flags

- Urgency, threats, or 'limited time' pressure
- Requests for passwords, MFA codes, gift cards, crypto, or wire transfers
- Links that look slightly wrong (misspellings, strange domains)
- Requests to install remote access tools

Official resources

[FTC: How To Recognize and Avoid Phishing Scams](#)

[FTC \(ES\): Como reconocer y evitar las estafas de phishing](#)

[FBI: Spoofing and Phishing](#)

[CISA: Recognize and Report Phishing](#)

Guía Detente Verifica Reporta

Un guion simple para phishing, smishing y llamadas de estafa.

3 steps

DETENTE

- No abras enlaces ni adjuntos.
- No respondas ni discutas con el estafador.
- Toma captura para evidencia.

VERIFICA

- Usa canales oficiales: escribe el sitio tú mismo o usa la app oficial.
- Llama a un número confiable (tarjeta, estado o sitio oficial).
- Pide ayuda a alguien de confianza si te presionan.

REPORTA

- Reenvía textos de estafa al SPAM (7726).
- Reporta en ReportFraud.ftc.gov (Español: ReporteFraude.ftc.gov).
- Reporta crimen cibernético en ic3.gov.

Guiones rápidos

Mensaje del banco: Recibí un mensaje sobre mi cuenta. Estoy llamando al número en mi tarjeta para verificar. ¿Puede confirmar si es real?

Delivery/texto con enlace: No abro enlaces en textos. Voy a revisar el tracking en la app/sitio oficial.

Soporte técnico pop-up/llamada: Yo no pedí soporte. Voy a cerrar esta ventana y contactar soporte por el sitio oficial.

Emergencia familiar: Voy a llamarte de vuelta al número guardado para confirmar.

Red flags

- Urgencia, amenazas o presión de 'tiempo limitado'
- Piden contraseñas, códigos MFA, gift cards, crypto o transferencias
- Enlaces raros (errores, dominios extraños)
- Piden instalar herramientas de acceso remoto

Recursos oficiales

[FTC: How To Recognize and Avoid Phishing Scams](#)

[FTC \(ES\): Como reconocer y evitar las estafas de phishing](#)

[FBI: Spoofing and Phishing](#)

[CISA: Recognize and Report Phishing](#)

Incident Response & Recovery Checklist (Home Users)

What to do first, what not to do, and where to report.

Do this first

- [] Disconnect from the internet (Wi-Fi off / unplug ethernet).
- [] Do NOT enter passwords on a device that may be compromised.
- [] From a clean device, change your email password and enable MFA.
- [] Check for suspicious logins and sign out of other sessions.
- [] Contact your bank/credit card if financial info may be exposed.
- [] Run a built-in security scan and apply updates.
- [] Restore from backups if needed (do not connect backups until you are ready).

What NOT to do

- Do not share MFA codes or passwords with anyone.
- Do not install remote-access tools because a caller told you to.
- Do not pay with gift cards, crypto, or wire transfers.
- Do not click 'fix now' pop-ups.

Save evidence

- Screenshot the message / pop-up.
- Save sender email/phone number, date/time, and any URLs.
- Keep receipts/transaction IDs if money was sent.

Where to report

- Report fraud at ReportFraud.ftc.gov (Spanish: ReporteFraude.ftc.gov).
- Report cyber-enabled crime at ic3.gov (FBI).
- If identity theft: consider IdentityTheft.gov steps.
- If immediate danger or threats: contact local law enforcement.

Official resources

ReportFraud.ftc.gov

ReporteFraude.ftc.gov (ES)

[IC3](https://ic3.gov) (FBI)

[CISA: Reporting a Cyber Incident](https://www.cisa.gov/incident-response)

Checklist de Respuesta y Recuperación (Hogar)

Qué hacer primero, qué NO hacer y dónde reportar.

Haz esto primero

- [] Desconecta internet (apaga Wi-Fi / desconecta cable).
- [] NO pongas contraseñas en un dispositivo posiblemente comprometido.
- [] Desde un dispositivo limpio, cambia password del email y activa MFA.
- [] Revisa inicios de sesión sospechosos y cierra otras sesiones.
- [] Contacta el banco/tarjeta si puede haber exposición financiera.
- [] Corre escaneo de seguridad y aplica updates.
- [] Restaura desde backups si hace falta (no conectes backups hasta estar listo).

Qué NO hacer

- No compartas códigos MFA ni contraseñas con nadie.
- No instales herramientas de acceso remoto porque alguien lo dice por teléfono.
- No pagues con gift cards, crypto o transferencias.
- No hagas clic en pop-ups de 'fix now'.

Save evidence

- Toma captura del mensaje / pop-up.
- Guarda email/número del remitente, fecha/hora y URLs.
- Guarda recibos/IDs de transacción si enviaste dinero.

Where to report

- Reporta fraude en ReportFraud.ftc.gov (Español: ReporteFraude.ftc.gov).
- Reporta crimen cibernético en ic3.gov (FBI).
- Si es robo de identidad: revisa pasos en IdentityTheft.gov.
- Si hay amenazas o peligro inmediato: contacta autoridades locales.

Recursos oficiales

ReportFraud.ftc.gov

ReporteFraude.ftc.gov (ES)

[IC3](https://ic3.gov) (FBI)

[CISA: Reporting a Cyber Incident](https://www.cisa.gov/reporting-a-cyber-incident)

Age-Tailored Cyber Safety Cards

Quick cards for family conversations. Print or screenshot.

Kids (Under 13)

- [] Ask a parent/guardian before clicking links or downloading games.
- [] Do not share your real name, address, school, or passwords online.
- [] If a message feels scary or urgent, STOP and show an adult.
- [] Only chat with people you know in real life (when possible).
- [] In games: ignore 'free coins/skins' links - those are often scams.

Script: Family script: "If you get a weird message, you will not be in trouble. Show me right away."

Remember: Stop / Verify / Report.

Age-Tailored Cyber Safety Cards

Teens

- [] Use MFA on social media and email.
- [] Watch for account recovery scams and fake 'support' DMs.
- [] Do not send private photos to strangers; sextortion scams are real.
- [] Check privacy settings and location sharing.
- [] Verify links before tapping - type the site yourself if possible.

Script: Friend check: "I got a strange message from you. I'm calling/texting you back to confirm."

Remember: Stop / Verify / Report.

Age-Tailored Cyber Safety Cards

Adults

- [] Secure email with MFA first (it resets other accounts).
- [] Use unique passwords and a password manager.
- [] Treat delivery, banking, job, and tech-support messages as suspicious until verified.
- [] Keep devices and router updated.
- [] Back up important files (photos, documents) and test restore.

Script: Rule: No one gets passwords, MFA codes, or remote access - period.

Remember: Stop / Verify / Report.

Age-Tailored Cyber Safety Cards

Older Adults

- [] Scammers may call pretending to be your bank, 'Microsoft', or government.
- [] Do not let anyone install remote-access tools or take control of your computer.
- [] If pressured, hang up. Call back using a trusted number (from card/statement).
- [] Ask a trusted family member to help verify suspicious requests.
- [] Use MFA and keep a written list of official support numbers.

Script: If it is urgent, it is probably a scam. Real support will let you verify calmly.

Remember: Stop / Verify / Report.

Tarjetas de Ciberseguridad por Edad

Tarjetas rápidas para conversaciones en familia. Imprime o guarda captura.

Niños (Menores de 13)

- [] Pide ayuda a un adulto antes de clicar enlaces o bajar juegos.
- [] No compartas tu nombre real, dirección, escuela o contraseñas en línea.
- [] Si un mensaje da miedo o mete prisa, DETENTE y enséñalo a un adulto.
- [] Chatea solo con gente que conoces en la vida real (cuando se pueda).
- [] En juegos: ignora enlaces de 'monedas/skins gratis' - suelen ser estafa.

Guion: Guion: "Si recibes un mensaje raro, no estás en problemas. Enséñame de inmediato."

Recuerda: Detente / Verifica / Reporta.

Tarjetas de Ciberseguridad por Edad

Adolescentes

- [] Activa MFA en redes sociales y email.
- [] Cuidado con estafas de recuperación de cuenta y DMs de 'soporte' falsos.
- [] No envíes fotos privadas a desconocidos; la extorsión existe.
- [] Revisa privacidad y compartir ubicación.
- [] Verifica enlaces antes de tocar - mejor escribe el sitio tú mismo.

Guion: Chequeo con amistad: "Me llegó un mensaje raro de ti. Te llamo/texteo para confirmar."

Recuerda: Detente / Verifica / Reporta.

Tarjetas de Ciberseguridad por Edad

Adultos

- [] Asegura el email con MFA primero (resetea otras cuentas).
- [] Usa contraseñas únicas y gestor de contraseñas.
- [] Trata mensajes de delivery, banca, trabajo y soporte como sospechosos hasta verificar.
- [] Mantén dispositivos y router actualizados.
- [] Haz backups de archivos importantes y prueba restaurar.

Guion: Regla: Nadie recibe contraseñas, códigos MFA, ni acceso remoto.

Recuerda: Detente / Verifica / Reporta.

Tarjetas de Ciberseguridad por Edad

Adultos Mayores

- [] Pueden llamar haciéndose pasar por el banco, 'Microsoft' o gobierno.
- [] No dejes que instalen herramientas de acceso remoto ni controlen tu computadora.
- [] Si te presionan, cuelga. Llama de vuelta con un número confiable (tarjeta/estado).
- [] Pide ayuda a un familiar de confianza para verificar.
- [] Usa MFA y guarda una lista escrita de números oficiales.

Guion: Si es 'urgente', probablemente es estafa. El soporte real te deja verificar con calma.

Recuerda: Detente / Verifica / Reporta.

Official resources / Recursos oficiales

[FTC: How To Avoid a Scam](#)

[FBI: Scams and Safety \(Common scams\)](#)

[CISA: Secure Our World](#)