



Household Digital Privacy & Fraud Prevention Toolkit

Practical, bilingual checklists for safer everyday tech use (EN/ES)

Kit de Privacidad Digital y Prevención de Fraude en el Hogar

What this toolkit is

A set of short sections you can print or use on-screen. Each section follows the same flow:

Learn → Do → Practice → Check.

Goal: reduce common home-user risks (fraud, account takeover, oversharing) with steps that are safe and realistic.

Safety promise

We will never ask for passwords, MFA codes, or logins.

If any "helper" requests those, treat it as a scam.

Prepared for: Zero Day Tech Labs

Author: Joseph R. Gonzalez Rios • Polytechnic University of Puerto Rico

Version 1.0 • January 2026

Quick Start + Contents

Use this page as your "where do I begin" map.

Quick Start (EN)

Pick one item per day. Small wins add up.

- [] Lock your phone number with a carrier PIN and enable port-out protection.
- [] Turn on purchase alerts for your bank and credit card.
- [] Run a privacy checkup (remove old public info and tighten social settings).
- [] Set family rules for chats, games, and app installs.

Inicio rápido (ES)

Escoge una cosa por día. Lo pequeño se vuelve grande.

- [] Asegura tu número con un PIN del proveedor móvil y activa protección contra port-out.
- [] Activa alertas de compra del banco y de la tarjeta.
- [] Haz un privacy checkup (borra info pública vieja y ajusta redes).
- [] Define reglas familiares para chats, juegos y descargas.

Contents

Mobile & Phone Number Protection (EN/ES)	3
Safer Shopping & Payments (EN/ES)	7
Privacy & Online Presence (EN/ES)	11
Family Online Safety Plan (EN/ES)	15
Appendix: Safe Device Handoff & Disposal (EN/ES)	19

Protect Your Phone Number & Mobile Accounts

Reduce the risk of account takeovers like SIM swap and port-out fraud.

Learn

Your phone number can unlock password resets, banking alerts, and social accounts.

If someone moves your number to a new SIM/eSIM (SIM swap) or transfers it to another carrier (port-out fraud), they may receive your calls and texts - including security codes.

- Your phone suddenly loses service or shows "SOS" only (and you did not change carriers).
- You get an alert about a SIM change or number transfer you did not request.
- Accounts start sending password reset emails or "new device" notices.
- Someone pressures you to "verify" a code they just texted you.

Do

- [] Add a carrier account PIN/passcode and ask about port-out protection (number transfer lock/freeze).
- [] Turn on carrier notifications for SIM change and number porting (if available).
- [] Move critical accounts away from SMS codes when possible (use an authenticator app or security key).
- [] Use a strong device passcode (6+ digits or alphanumeric) and enable Face ID/Touch ID.
- [] Enable "Find My" (or equivalent) and confirm you can locate your device.
- [] Turn on automatic OS updates and remove apps you do not use.
- [] Review app permissions for Location, Microphone, and Camera. Keep "Always" access rare.

Protect Your Phone Number & Mobile Accounts

Reduce the risk of account takeovers like SIM swap and port-out fraud.

Practice

- Carrier check (5 min): Log in to your mobile account and confirm your PIN is set. Find the support page for port-out protection and bookmark it.
- Permission audit (10 min): Pick 5 apps. If they do not need Location/Mic/Camera, set access to "Never" or "While Using".
- Lost-phone drill (2 min): Use "Find My" to play a sound or show the phone on a map. Confirm your recovery email is current.

Check

- ☐ My carrier account has a PIN/passcode.
- ☐ Port-out protection is enabled (or I know exactly how to turn it on).
- ☐ SIM-change alerts are on.
- ☐ My device uses a strong passcode and biometrics.
- ☐ "Find My" is enabled and tested.
- ☐ I reviewed app permissions in the last 30 days.

Official resources

[FTC: SIM swap scams - how to protect yourself](#)

[FCC: Port-out fraud scam alert](#)

[CISA: Mobile communications best practices \(PDF\)](#)

[NSA: Mobile device best practices \(PDF\)](#)

Protege tu número de teléfono y tus cuentas móviles

Reduce el riesgo de tomar control de cuentas, como SIM swap y fraude de port-out.

Aprende

Tu número de teléfono puede abrir puertas: reseteos de contraseña, alertas del banco y cuentas sociales.

Si alguien mueve tu número a otra SIM/eSIM (SIM swap) o lo transfiere a otra compañía (port-out), puede recibir tus llamadas y textos - incluyendo códigos de seguridad.

- Tu teléfono se queda sin servicio o muestra "SOS" (y tú no cambiaste de compañía).
- Te llega un aviso de cambio de SIM o transferencia del número que no pediste.
- Tus cuentas empiezan a mandar reseteos de contraseña o avisos de "nuevo dispositivo".
- Alguien te presiona para que "verifiques" un código que acaba de llegar por texto.

Haz

- [] Pon un PIN/contraseña en tu cuenta con la compañía móvil y pregunta por protección contra port-out (bloqueo de transferencia del número).
- [] Activa notificaciones para cambio de SIM y transferencia del número (si existe).
- [] Saca cuentas críticas de códigos por SMS cuando se pueda (mejor app autenticadora o llave).
- [] Usa un passcode fuerte (6+ dígitos o alfanumérico) y activa Face ID/Touch ID.
- [] Activa "Find My" (o equivalente) y confirma que puedes localizar el dispositivo.
- [] Activa actualizaciones automáticas y elimina apps que no uses.
- [] Revisa permisos de Ubicación, Micrófono y Cámara. El acceso "Siempre" debe ser raro.

Protege tu número de teléfono y tus cuentas móviles

Reduce el riesgo de tomar control de cuentas, como SIM swap y fraude de port-out.

Practica

- Chequeo con la compañía (5 min): Entra a tu cuenta y confirma que el PIN está puesto. Busca la página del bloqueo de transferencia y guárdala.
- Auditoría de permisos (10 min): Escoge 5 apps. Si no necesitan Ubicación/Mic/Cámara, ponlo en "Nunca" o "Solo al usar".
- Simulacro (2 min): Usa "Find My" para sonar o ubicar el teléfono. Verifica que tu email de recuperación está al día.

Verifica

- ☐ Mi cuenta con la compañía móvil tiene PIN/contraseña.
- ☐ La protección contra port-out está activa (o sé exactamente cómo activarla).
- ☐ Alertas de cambio de SIM activas.
- ☐ Mi dispositivo usa passcode fuerte y biometría.
- ☐ "Find My" está activo y probado.
- ☐ Revisé permisos de apps en los últimos 30 días.

Recursos oficiales

[FTC: SIM swap scams - how to protect yourself](#)

[FCC: Port-out fraud scam alert](#)

[CISA: Mobile communications best practices \(PDF\)](#)

[NSA: Mobile device best practices \(PDF\)](#)

Safer Online Shopping, Banking, and Payments

Protect your money without making shopping feel like a final exam.

Learn

Most payment fraud succeeds because it creates urgency: "last chance," "package problem," "confirm now," or "pay today." A calm 30-second pause is a security control.

Common scam patterns:

- Look-alike stores and "sponsored" ads that lead to fake checkout pages.
- Delivery texts that ask you to click a link or pay a small fee.
- Someone insists you pay with gift cards, wire transfer, or cryptocurrency.
- A seller pushes you to "move the conversation" off the platform.

Do

- [] Pay by credit card when possible (stronger protections than debit).
- [] Never pay with gift cards, wire transfer, or crypto when someone demands it.
- [] Type the website yourself for logins and payments; avoid clicking checkout links from texts.
- [] Use official apps for banks/retailers when you can, and turn on purchase alerts.
- [] Review bank and card statements weekly (set a calendar reminder).
- [] Use a separate email for shopping accounts (optional, but helpful).
- [] For deliveries: track in the official app/site (USPS/FedEx/UPS) instead of text links.

Safer Online Shopping, Banking, and Payments

Protect your money without making shopping feel like a final exam.

Practice

- Deal sanity check: Before you buy, search "store name + scam" and read the return policy. If it feels messy, walk away.
- Shipping text drill: If you get a delivery text, do not click. Open the official carrier site/app and enter the tracking number yourself.
- If you already paid: Contact your bank/card provider right away and report the scam to [ReportFraud.ftc.gov](https://reportfraud.ftc.gov).

Check

- ☐ I do not pay strangers with gift cards, wire transfer, or crypto.
- ☐ I use transaction alerts for my bank/card.
- ☐ I verify delivery issues using official carrier sites/apps.
- ☐ I check statements weekly.
- ☐ I can explain "sponsored ad" risk to someone else.
- ☐ I know where to report scams ([ReportFraud.ftc.gov](https://reportfraud.ftc.gov)).

Official resources

[FTC: Online shopping tips](#)

[FTC: Gift card scams](#)

[CFPB: Play it safe online](#)

[USPIS: Package tracking text scams \(smishing\)](#)

[FTC: Report a scam](#)

Compras y pagos en línea más seguros

Protege tu dinero sin que comprar se sienta como un examen final.

Aprende

La mayoría del fraude funciona por urgencia: "última oportunidad," "problema con el paquete," "confirma ahora" o "paga hoy." Una pausa de 30 segundos es un control de seguridad.

Patrones comunes:

- Tiendas falsas parecidas a las reales y anuncios "patrocinados" que llevan a checkouts falsos.
- Textos de entrega que te piden clicar un enlace o pagar una tarifa pequeña.
- Alguien insiste que pagues con gift cards, wire transfer o criptomoneda.
- Un vendedor te empuja a "mover la conversación" fuera de la plataforma.

Haz

- [] Paga con tarjeta de crédito cuando se pueda (mejor protección que débito).
- [] Nunca pagues con gift cards, wire transfer o crypto cuando alguien lo exige.
- [] Escribe el sitio tú mismo para logins y pagos; evita links de checkout en textos.
- [] Usa apps oficiales de banco/tiendas y activa alertas de compra.
- [] Revisa estados de cuenta cada semana (pon recordatorio).
- [] Usa un email separado para compras (opcional, pero ayuda).
- [] Para entregas: rastrea en la app/sitio oficial (USPS/FedEx/UPS), no en enlaces por texto.

Compras y pagos en línea más seguros

Protege tu dinero sin que comprar se sienta como un examen final.

Practica

- Chequeo rápido: Antes de comprar, busca "nombre de la tienda + scam" y lee la política de devolución. Si se ve raro, no compres.
- Drill de textos: Si llega un texto de entrega, no cliques. Abre el sitio/app oficial y entra el tracking tú mismo.
- Si ya pagaste: Llama al banco/tarjeta de inmediato y reporta en ReportFraud.ftc.gov.

Verifica

- ☐ No pago a extraños con gift cards, wire transfer o crypto.
- ☐ Uso alertas de transacciones del banco/tarjeta.
- ☐ Verifico problemas de entrega en sitios/apps oficiales.
- ☐ Reviso estados de cuenta semanalmente.
- ☐ Puedo explicar el riesgo de anuncios "patrocinados".
- ☐ Sé dónde reportar estafas (ReportFraud.ftc.gov).

Recursos oficiales

[FTC: Online shopping tips](#)

[FTC: Gift card scams](#)

[CFPB: Play it safe online](#)

[USPIS: Package tracking text scams \(smishing\)](#)

[FTC: Report a scam](#)

Privacy and Managing Your Online Presence

Share less, control more, and make account recovery harder for criminals.

Learn

Attackers often start with public information: your phone number, birthday, employer, and "security question" clues.

Privacy is not hiding. It is controlling what is shared and with whom.

- Data brokers and old profiles can expose addresses and phone numbers.
- Oversharing makes account recovery and impersonation easier for scammers.
- Ad settings and location history can reveal routines.
- A quick privacy checkup can remove years of accidental sharing.

Do

- [] Run a privacy checkup for your main accounts (Google, Apple, Microsoft, etc.).
- [] Remove your phone number and home address from public profiles when possible.
- [] Review who can see your posts, friends list, and tagged photos.
- [] Turn off location sharing you do not use; limit "always on" location access.
- [] Set account recovery options you control (recovery email + phone) and keep them current.
- [] Search your name and username online once a quarter and clean up old accounts.

Privacy and Managing Your Online Presence

Share less, control more, and make account recovery harder for criminals.

Practice

- 15-minute privacy sweep: Search your name. If you find old profiles, either delete them or lock them down.
- Social media quick lock: Set profile visibility to friends-only and hide your friends list (if the platform allows).
- Location audit: Turn off location history if you do not need it. Keep navigation apps "while using".

Check

- ☐ I ran a privacy checkup for at least one major account this month.
- ☐ My phone number is not posted publicly.
- ☐ Location sharing is limited to what I actually use.
- ☐ My recovery email/phone are current.
- ☐ I know what shows up when I search my name.
- ☐ I reviewed social media privacy settings in the last 90 days.

Official resources

[FTC: Protecting your privacy online](#)

[CISA: Manage your online presence](#)

[CISA: Social media account protection guide \(PDF\)](#)

[Google: Privacy Checkup](#)

Privacidad y manejo de tu presencia en línea

Comparte menos, controla más y haz más difícil la recuperación de cuentas para estafadores.

Aprende

Muchos ataques empiezan con información pública: tu número, cumpleaños, trabajo y pistas para "preguntas de seguridad".

Privacidad no es esconderse. Es controlar qué se comparte y con quién.

- Data brokers y perfiles viejos pueden exponer dirección y teléfono.
- Compartir demasiado facilita suplantación y resets de cuenta.
- Ajustes de anuncios e historial de ubicación pueden revelar rutinas.
- Un privacy checkup rápido puede borrar años de compartir sin querer.

Haz

- [] Haz un privacy checkup en tus cuentas principales (Google, Apple, Microsoft, etc.).
- [] Quita tu número y dirección de perfiles públicos cuando se pueda.
- [] Revisa quién ve tus posts, lista de amigos y fotos etiquetadas.
- [] Apaga ubicación que no uses; limita acceso "Siempre".
- [] Configura opciones de recuperación (email + teléfono) y mantenlas al día.
- [] Busca tu nombre y usuario en internet cada trimestre y cierra cuentas viejas.

Privacidad y manejo de tu presencia en línea

Comparte menos, controla más y haz más difícil la recuperación de cuentas para estafadores.

Practica

- Barrido de 15 min: Busca tu nombre. Si salen perfiles viejos, bórralos o ciérralos.
- Candado rápido: Pon el perfil en "solo amigos" y esconde la lista de amigos (si la app lo permite).
- Auditoría de ubicación: Apaga historial si no lo necesitas. Deja apps de mapa en "solo al usar".

Verifica

- ☐ Hice un privacy checkup en al menos una cuenta grande este mes.
- ☐ Mi número no está publicado.
- ☐ La ubicación se comparte solo cuando lo necesito.
- ☐ Email/teléfono de recuperación están al día.
- ☐ Sé qué aparece cuando busco mi nombre.
- ☐ Revisé privacidad de redes en los últimos 90 días.

Recursos oficiales

[FTC: Protecting your privacy online](#)

[CISA: Manage your online presence](#)

[CISA: Social media account protection guide \(PDF\)](#)

[Google: Privacy Checkup](#)

Family Online Safety Plan (Kids and Teens)

Clear rules, calm conversations, and settings that match your family's reality.

Learn

Kids do not need perfect tech. They need repeatable habits and an adult they can talk to.

The biggest risks usually come from: strangers in chats, pressure to share photos, and "free" offers that steal accounts or money.

- Gaming and group chats can include adults pretending to be kids.
- "Free skins / free currency" offers often lead to stolen logins.
- Oversharing (school name, schedule, location) makes targeting easier.
- Parental controls work best when paired with family rules.

Do

- [] Create a family rule: no sharing real name, school, address, or phone number in chats.
- [] Agree on a "pause word" kids can use when something feels wrong (no trouble, just help).
- [] Turn on parental controls for devices and consoles (content ratings, purchases, screen time).
- [] Set purchasing rules: no in-app purchases without an adult.
- [] Keep devices updated and install apps only from official stores.
- [] Do a monthly 10-minute check-in: new apps, new friends, any weird messages.

Family Online Safety Plan (Kids and Teens)

Clear rules, calm conversations, and settings that match your family's reality.

Practice

- Role-play (2 min): A stranger offers free game currency. Practice: "No thanks" + block + tell an adult.
- Screenshot habit: If a message feels creepy or urgent, take a screenshot and stop responding.
- Family agreement: Write down 3 rules and put them near the charging station.

Check

- ☐ We have 3 clear family rules for online behavior.
- ☐ Parental controls are enabled for purchases and age-appropriate content.
- ☐ Kids know they can ask for help without getting in trouble.
- ☐ We do a monthly check-in on apps and contacts.
- ☐ We know where to report exploitation or serious concerns.
- ☐ We treat "free" offers and giveaways as suspicious by default.

Official resources

[FTC: How to use parental controls](#)

[FTC: Protecting kids online](#)

[CISA: Keeping children safe online](#)

[NCMEC: NetSmartz resources for families](#)

[FBI: Safe Online Surfing \(SOS\) program](#)

Plan familiar de seguridad en línea (niños y adolescentes)

Reglas claras, conversaciones tranquilas y ajustes que encajan con tu familia.

Aprende

Los niños no necesitan tecnología perfecta. Necesitan hábitos repetibles y un adulto con quien hablar.

Los riesgos más comunes: extraños en chats, presión para compartir fotos y ofertas "gratis" que roban cuentas o dinero.

- En juegos y chats puede haber adultos fingiendo ser menores.
- Ofertas de "skins gratis" o "monedas gratis" suelen robar logins.
- Compartir escuela, horarios o ubicación facilita que los apunten.
- Parental controls funcionan mejor si hay reglas en casa.

Haz

- [] Regla familiar: no compartir nombre real, escuela, dirección ni teléfono en chats.
- [] Acordar una "palabra de pausa" para pedir ayuda sin miedo a regaños.
- [] Activa parental controls en dispositivos y consolas (ratings, compras, tiempo).
- [] Reglas de compras: nada de in-app purchases sin un adulto.
- [] Actualizaciones al día y apps solo de tiendas oficiales.
- [] Cada mes: check-in de 10 min (apps nuevas, contactos nuevos, mensajes raros).

Plan familiar de seguridad en línea (niños y adolescentes)

Reglas claras, conversaciones tranquilas y ajustes que encajan con tu familia.

Practica

- Role-play (2 min): Un extraño ofrece moneda gratis. Practica: "No" + bloquear + avisar a un adulto.
- Hábito de evidencia: Si un mensaje se siente creepy o urgente, toma screenshot y no respondas.
- Acuerdo familiar: Escribe 3 reglas y ponlas cerca del área de carga.

Verifica

- ☐ Tenemos 3 reglas claras para comportamiento en línea.
- ☐ Parental controls están activos para compras y contenido por edad.
- ☐ Los niños saben que pueden pedir ayuda sin castigo.
- ☐ Hacemos un check-in mensual de apps y contactos.
- ☐ Sabemos dónde reportar explotación o preocupaciones serias.
- ☐ Tratamos ofertas "gratis" como sospechosas por default.

Recursos oficiales

[FTC: How to use parental controls](#)

[FTC: Protecting kids online](#)

[CISA: Keeping children safe online](#)

[NCMEC: NetSmartz resources for families](#)

[FBI: Safe Online Surfing \(SOS\) program](#)

Appendix: Safe Device Handoff and Secure Disposal

Before you sell, donate, recycle, or give a device to family.

- ☐ Back up important photos and files.
- ☐ Sign out of accounts (email, iCloud/Google, app stores).
- ☐ Remove SIM and SD cards (or erase eSIM if needed).
- ☐ Turn off device tracking locks (Find My / Factory Reset Protection) only after you are ready to wipe.
- ☐ Factory reset the device using the official settings menu.
- ☐ If possible, update the device before resetting (helps security and reliability).
- ☐ Recycle using trusted programs; keep receipts when available.

Official resources

[FTC: Remove personal info from your phone](#)

[FTC: Remove personal info before getting rid of a computer](#)

[Apple: What to do before you sell or give away your iPhone/iPad](#)

[Google: Reset your Android device to factory settings](#)

Apéndice: entrega segura y desecho de dispositivos

Antes de vender, donar, reciclar o pasar un dispositivo a alguien.

- [] Haz backup de fotos y archivos importantes.
- [] Cierra sesión en cuentas (email, iCloud/Google, tiendas de apps).
- [] Quita SIM y SD (o borra eSIM si aplica).
- [] Apaga bloqueos anti-robo (Find My / Factory Reset Protection) solo cuando ya estés listo para borrar.
- [] Haz factory reset desde el menú oficial de ajustes.
- [] Si puedes, actualiza el dispositivo antes de resetear (mejora seguridad y estabilidad).
- [] Recicla con programas confiables y guarda recibos si existen.

Recursos oficiales

[FTC: Remove personal info from your phone](#)

[FTC: Remove personal info before getting rid of a computer](#)

[Apple: What to do before you sell or give away your iPhone/iPad](#)

[Google: Reset your Android device to factory settings](#)