GUÍA DEL TOOLKIT
Español

ZERODAY
TECH LABS

Kit de seguridad cibernética para el hogar

Una guía completa en español con listas prácticas para el hogar.

Audiencia	Familias, adultos mayores, niños, cuidadores y ayudantes comunitarios.
Propósito	Reunir las guías principales de seguridad del hogar en un solo documento.
Mejor uso	Úsala como Toolkit principal impreso para talleres y referencia familiar.

Comienza con estas acciones

[ ]	Protege primero el correo electrónico porque permite recuperar muchas otras cuentas.
[ ]	Usa una contraseña larga y diferente para correo, banco y cuenta del proveedor móvil.
[ ]	Activa autenticación multifactor en correo, banco, redes sociales y cuentas en la nube.
[ ]	Activa actualizaciones automáticas en teléfonos, computadoras, navegadores y aplicaciones.
[ ]	No abras enlaces en mensajes sorpresa de banco, paquete, premio o soporte.
[ ]	Pregunta a una persona de confianza antes de enviar dinero, códigos, contraseñas o tarjetas de regalo.

Regla familiar

Si un mensaje crea miedo, presión o secreto, pausa antes de actuar. Un servicio real debe permitir verificar con calma.

Próximo paso

Abre la lista básica y la guía detener verificar reportar. Convierten este inicio rápido en una rutina del hogar.

Router y Wi Fi

[ ]	Cambia la contraseña de administrador del router.
[ ]	Usa WPA3 o WPA2 WPA3 si está disponible.
[ ]	Apaga WPS si el hogar no lo usa.
[ ]	Apaga el acceso remoto de administración si no es necesario.
[ ]	Crea Wi Fi de invitados para visitas y dispositivos inteligentes cuando sea posible.

Cuentas y dispositivos

[ ]	Protege el correo con autenticación multifactor.
[ ]	Usa contraseñas diferentes para cuentas importantes.
[ ]	Activa actualizaciones en teléfonos, computadoras, navegadores y aplicaciones.
[ ]	Elimina aplicaciones y extensiones que no uses.
[ ]	Haz respaldo de fotos y documentos importantes.

Revisión

Haz una revisión corta cada tres meses. Revisa actualizaciones, contraseñas, respaldos y dispositivos desconocidos.

Detener

[ ]	No hagas clic en enlaces.
[ ]	No abras archivos adjuntos.
[ ]	No respondas al remitente.
[ ]	No compartas contraseñas, códigos ni datos de pago.
[ ]	Toma una captura si es seguro.

Verificar

[ ]	Usa el sitio o aplicación oficial que ya conoces.
[ ]	Llama a un número confiable de una tarjeta, estado de cuenta o sitio oficial.

[ ]	Pregunta a un familiar o ayudante de confianza.
[ ]	Revisa si el mensaje crea miedo o urgencia.

Reportar

[ ]	Reenvía textos de estafa al 7726 cuando esté disponible.
[ ]	Reporta fraude en ReportFraud.ftc.gov.
[ ]	Reporta crimen por internet en IC3.gov cuando aplique.
[ ]	Reporta robo de identidad en IdentityTheft.gov.

Haz esto primero

[ ]	Desconecta el dispositivo sospechoso de internet si es necesario.
[ ]	No escribas contraseñas nuevas en un dispositivo que puede estar comprometido.
[ ]	Desde un dispositivo limpio, cambia primero la contraseña del correo.
[ ]	Activa autenticación multifactor.
[ ]	Revisa accesos recientes y cierra sesiones desconocidas.
[ ]	Llama al banco o tarjeta si puede haber datos de pago o dinero involucrado.

Limpiar y recuperar

[ ]	Ejecuta una revisión de seguridad integrada.
[ ]	Aplica actualizaciones.
[ ]	Elimina aplicaciones o extensiones sospechosas.
[ ]	Restaura archivos desde respaldo si es necesario.
[ ]	Guarda capturas y notas para reportar.

No hagas esto

[ ]	No compartas códigos con una persona que llama.
[ ]	No permitas acceso remoto porque una ventana emergente lo pidió.
[ ]	No pagues a un extraño que dice que puede quitar un virus.

Niños

[ ]	Pregunta a un adulto de confianza antes de hacer clic o descargar juegos.
[ ]	No compartas nombre real, dirección, escuela, fotos o contraseñas en línea.
[ ]	Si un mensaje da miedo o parece urgente, muéstralo a un adulto.

Adolescentes

[ ]	Usa autenticación multifactor en correo, escuela, juegos y redes sociales.
[ ]	No repitas contraseñas.
[ ]	No envíes fotos privadas a personas desconocidas.
[ ]	Revisa privacidad y ubicación compartida.

Adultos

[ ]	Protege primero el correo.
[ ]	Usa contraseñas únicas y un gestor de contraseñas.
[ ]	Trata mensajes de entrega, banco, empleo y soporte como sospechosos hasta verificar.
[ ]	Haz respaldo de archivos importantes.

Adultos mayores

[ ]	No confíes en llamadas sorpresa sobre virus, reembolsos, cuentas bloqueadas, tarjetas de regalo o emergencias.
[ ]	Cuelga y llama usando un número confiable.
[ ]	No permitas que una persona controle tu computadora.
[ ]	Pregunta a alguien de confianza antes de enviar dinero o códigos.

Mantén esta guía cerca del dispositivo o cuenta que protege. Los hábitos pequeños hacen una diferencia real cuando se repiten.