Semana 2: Todo lo que aprendiste sobre ciberseguridad en familia

Subtítulo: Seis lecturas que cambian la forma en que ves tu móvil, tu WiFi, tu WhatsApp y la seguridad de los tuyos.

Si llegaste aquí por primera vez, bienvenido. Si ya llevas unos días leyendo este blog, sabe que lo que vas a encontrar no es un repaso técnico ni un titular de alarma. Es algo diferente: un espacio donde se analiza la seguridad digital como lo que realmente es en 2026: una cuestión cultural, no tecnológica.

Esta semana publicamos seis artículos que, vistos juntos, forman algo más que una lista de consejos. Forman un mapa. Un mapa de los puntos donde tu vida digital —y la de tu familia o tu negocio— es más vulnerable de lo que crees, y de por qué cada uno de esos puntos no falla por negligencia, sino por confianza.

Aquí tienes el resumen. Cada sección enlaza al artículo completo por si quieres profundizar.

Aplicaciones que espían: qué permisos le das a tu móvil

Empezamos por el dispositivo que más datos sabe de ti en este momento: tu teléfono. No el ordenador del trabajo, no el servidor de la empresa. Tu móvil.

La mayoría de aplicaciones que instalamos —incluso las aparentemente inocuas— solicitan permisos que van mucho más allá de lo que necesitan para funcionar. Acceso al micrófono para una app de linterna. Acceso a los contactos para una calculadora. Lectura del historial de llamadas para un juego gratuito. No son errores de diseño: son decisiones deliberadas de recopilación de datos.

En este artículo analizamos cómo funciona la economía de los permisos, qué tipo de datos se venden o se comparten, y qué puedes revisar hoy mismo en los ajustes de tu dispositivo para limitar la exposición. No se trata de desinstalar todo. Se trata de entender qué está pasando y decidir de forma consciente.

Concepto clave: Economía de datos · Permisos silenciosos · Seguimiento pasivo

El proveedor que se convirtió en la puerta de entrada

Uno de los artículos más estratégicos de la semana. Y también uno de los más ignorados en el mundo de las pymes.

Los ataques a través de la cadena de suministro no son ciencia ficción ni exclusivos de grandes corporaciones. Son, en 2026, una de las vías de entrada más comunes en negocios medianos y pequeños. La lógica es simple: si el objetivo tiene buenas defensas, los criminales no atacan al objetivo. Atacan a quien tiene acceso al objetivo.

Tu gestoría. Tu proveedor de software. La empresa que gestiona tu web. La agencia que accede a tus redes sociales. Todos ellos pueden ser, sin saberlo, el eslabón más débil de tu cadena. Este artículo explica cómo ocurre, con un caso representativo, y qué controles básicos puede implementar cualquier negocio para reducir ese riesgo sin invertir en tecnología cara.

Concepto clave: Cadena de suministro digital · Control de accesos · Principio de mínimo privilegio

WiFi pública: lo que pasa cuando te conectas en un café

Cada vez que te conectas a una red WiFi abierta —en un aeropuerto, una cafetería, un hotel— estás tomando una decisión de seguridad, aunque no lo parezca. Y la mayoría de las veces, se toma sin pensar.

Este artículo desmonta varios mitos sobre las redes públicas y explica con claridad qué puede ver realmente alguien en tu misma red, qué tipo de ataques son factibles (y cuáles son exagerados), y por qué el riesgo no desaparece aunque la web que visites tenga el candado verde de HTTPS.

También analizamos el fenómeno de los "puntos de acceso falsos": redes con nombres convincentes creadas expresamente para capturar tráfico. Si alguna vez te has conectado a una WiFi llamada "CaféLibre" o "HotelGuest", este artículo te interesa.

Concepto clave: Man-in-the-middle · Redes trampa · Interceptación de tráfico

Estafas por WhatsApp: los mensajes que parecen de tu familia

Este es el artículo que más se compartió esta semana, y no es casualidad.

Las estafas a través de WhatsApp han alcanzado en 2026 un nivel de sofisticación que hace muy difícil distinguirlas de comunicaciones legítimas. No hablamos de mensajes en inglés con errores de ortografía. Hablamos de mensajes que conocen tu nombre, que mencionan a personas reales de tu entorno, que imitan el tono y el estilo de escritura de alguien cercano, y que crean una urgencia emocional que anula el pensamiento crítico.

El artículo analiza los patrones más frecuentes —el hijo que necesita dinero urgente, el familiar en apuros, el contacto que cambió de número— y explica el mecanismo psicológico detrás de cada uno. Porque entender por qué funciona es más útil que memorizar una lista de señales de alerta.

Concepto clave: Ingeniería social · Urgencia emocional · Suplantación de identidad

Ransomware: cuando enciendes el ordenador y todo ha desaparecido

Pocos escenarios generan más impacto que este: encender el ordenador un lunes por la mañana y encontrar todos los archivos cifrados. Un mensaje en pantalla. Una dirección de pago. Un plazo.

El ransomware no es nuevo, pero en 2026 ha evolucionado de forma que lo hace más dañino que en años anteriores. Ya no solo cifra: primero extrae. Primero roba tus datos, tus facturas, los datos de tus clientes. Y luego amenaza con publicarlos si no pagas. Es una doble extorsión que convierte cada ataque en una crisis de reputación además de una pérdida operativa.

Este artículo explica cómo entra el ransomware —normalmente por un correo, no por una vulnerabilidad técnica sofisticada—, qué ocurre en cada fase del ataque, y cuál es la única medida realmente efectiva que cualquier persona o empresa puede implementar hoy, sin presupuesto y sin conocimientos técnicos.

Concepto clave: Doble extorsión · Vector de entrada · Copia de seguridad offline

Cómo un desconocido puede saber dónde estudia tu hijo en menos de 3 minutos

Este es el artículo más incómodo de la semana. Y probablemente el más necesario.

El OSINT —Open Source Intelligence, o inteligencia de fuentes abiertas— es la técnica que usan los analistas de seguridad, los investigadores y, también, los actores maliciosos para recopilar información sobre una persona usando únicamente datos públicos. Sin hackear nada. Sin acceder a ningún sistema privado. Solo con lo que tú, sin saberlo, has dejado visible.

En este artículo simulamos el proceso desde cero: qué puede descubrir alguien con solo el nombre de tu hijo y acceso a redes sociales. El resultado, en la mayoría de los perfiles que analizamos, es perturbador. Nombre del colegio, horarios habituales, barrio de

residencia, actividades extraescolares, incluso el aspecto físico detallado. Todo en menos de tres minutos. Todo sin violar ninguna ley.

La reflexión no es que Internet sea peligroso. Es que la privacidad no es un ajuste técnico: es una práctica activa.

Concepto clave: OSINT · Huella digital · Privacidad activa · Protección de menores

Lo que conecta los seis artículos: el patrón que nadie te enseñó

Si lees estos seis artículos con distancia, hay algo que los atraviesa a todos. No es la tecnología. No son las vulnerabilidades técnicas ni el código malicioso. Es la confianza, la visibilidad y la normalización.

Confiamos en las apps que instalamos porque tienen millones de descargas. Confiamos en el WiFi del café porque tiene contraseña. Confiamos en el mensaje de WhatsApp porque viene de un número conocido. Tenemos visibilidad total sobre nuestras vidas en redes sociales porque nos parece normal compartirla. Y precisamente porque nos parece normal, no lo cuestionamos.

Los ataques que analizamos esta semana no necesitan romper nada. Solo necesitan que tú sigas haciendo lo que siempre has hecho.

El conocimiento no va a hacer que uses internet de forma paranoica. Va a hacer que uses internet de forma consciente. Y esa diferencia, multiplicada por millones de personas, cambia radicalmente el ecosistema de amenazas.

Tu próximo paso esta semana

No hace falta que hagas todo a la vez. Elige uno de estos seis artículos —el que más resuene contigo o con tu situación— y aplica una sola cosa de lo que propone. Solo una. Revisar los permisos de tres apps. Hablar con tu hijo sobre lo que comparte online. Crear una copia de seguridad offline.

La cultura de seguridad no se construye en un día. Se construye con decisiones pequeñas, repetidas en el tiempo.

¿Cuál de estos seis artículos te ha resultado más útil o más sorprendente? Cuéntalo en los comentarios. Y si conoces a alguien —un familiar, un compañero de trabajo, un amigo con hijos— a quien le vendría bien leer alguno de estos temas, comparte. Una persona informada es una persona más difícil de engañar.

Visita el blog para acceder a todos los recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero