Por qué la ciberseguridad empieza en casa (y no en la empresa)

Las empresas blindan sus sistemas. Pero cuando sus empleados llegan a casa, la puerta está abierta.

Hay una paradoja que pocas empresas quieren reconocer en voz alta: invierten miles de euros en firewalls, auditorías de seguridad y formación corporativa, pero cada tarde, cuando sus empleados apagan el ordenador de trabajo y encienden el portátil de casa, todo ese esfuerzo queda expuesto a través de una red wifi con contraseña de fábrica, una cuenta de correo compartida con el resto de la familia y un hijo de doce años que descarga juegos de sitios que nadie debería visitar.

La ciberseguridad real no empieza en el departamento de IT. Empieza en el salón de casa.

El eslabón que nadie protege

Las organizaciones llevan años construyendo capas de protección técnica cada vez más sofisticadas. Y aun así, el vector de ataque más utilizado por los ciberdelincuentes en 2026 sigue siendo el mismo de siempre: la persona. No el sistema. No el servidor. La persona.

Un empleado que en el trabajo sabe detectar un correo sospechoso puede, esa misma noche, hacer clic en un enlace fraudulento desde su cuenta personal porque el mensaje llegó a las 11 de la noche, estaba cansado y tenía el aspecto exacto de una notificación de paquete pendiente de entrega. El contexto cambia el comportamiento. Y en casa, el contexto es relajación, no vigilancia.

Esto no es un problema de inteligencia ni de formación técnica. Es un problema de cultura. De hábito. Y los hábitos se forman en el entorno más cotidiano que existe: el hogar.

Cuando la amenaza entra por la puerta de casa

Existe una falsa sensación de seguridad que puede resultar especialmente peligrosa: creer que los ciberdelincuentes solo atacan a quien tiene algo valioso que robar. En 2026, esa lógica está completamente invertida.

Los ataques más frecuentes no van dirigidos a grandes corporaciones con bases de datos millonarias. Van dirigidos a personas normales porque son más accesibles, menos preparadas y, en muchos casos, una puerta de entrada indirecta hacia objetivos más grandes. Un autónomo que gestiona las facturas de tres empresas medianas. Un contable que trabaja en remoto. Un padre que usa el mismo correo para el trabajo y para la cuenta del colegio de sus hijos.

La información que publicamos en redes sociales, los dispositivos conectados que acumulamos sin pensar, las contraseñas que reutilizamos por comodidad... todo eso construye un perfil que alguien, en algún lugar, puede usar en nuestra contra. Y lo más perturbador es que ni siquiera necesitan hackear ningún sistema para empezar: a menudo les basta con observar.

La seguridad digital como hábito familiar

Cuando hablamos de seguridad vial, no decimos que es un problema del fabricante del coche. Decimos que hay que abrocharse el cinturón, respetar los límites de velocidad y no coger el móvil al volante. Son hábitos que aprendemos, que enseñamos a nuestros hijos y que practicamos sin pensar porque los hemos integrado como parte de nuestra cultura cotidiana.

Con la seguridad digital debería funcionar exactamente igual, y todavía no funciona así.

La mayoría de las familias no ha hablado nunca de qué hacer si reciben una llamada de alguien que dice ser un familiar en apuros. Nunca han acordado cómo verificar que un mensaje de voz es real. Nunca han revisado juntos qué información personal está visible en las redes sociales de sus hijos. No porque no les importe, sino porque nadie les ha explicado que eso también forma parte de su seguridad.

Cambiar eso no requiere ser un experto en tecnología. Requiere información, conversación y unos pocos protocolos sencillos que, una vez incorporados, se vuelven automáticos.

Lo que nos estamos perdiendo (y lo que viene)

Hay amenazas concretas que hoy afectan a familias y pequeños negocios de formas que muchos todavía no imaginan. Ataques diseñados específicamente para explotar la confianza, la urgencia y los vínculos emocionales más cercanos. Herramientas que permiten imitar voces conocidas, construir mensajes sin errores ni señales de alarma, o acceder a sistemas enteros a través del proveedor menos esperado.

Cada uno de esos vectores tiene una respuesta práctica. No es magia y tampoco requiere invertir en tecnología. Requiere entender cómo funciona el engaño y tener una forma acordada de verificar antes de actuar.

Estoy preparando una guía gratuita que cubre exactamente eso: los ataques más relevantes de 2026, explicados sin tecnicismos, con ejemplos reales y protocolos concretos para familias y pequeños negocios.

Isaac Ruiz Romero.