2025: El Año en que la Ciberseguridad Dejó de Ser Cosa de Expertos

Por qué este año ha cambiado las reglas del juego digital para familias, empresas y usuarios de a pie.

Ya no se trata de si te van a atacar

Hay una frase que repito constantemente en mis formaciones y que, con cada año que pasa, resulta más difícil de rebatir: *"La pregunta no es si te van a atacar, sino cuándo y cómo"*. Durante mucho tiempo, esa afirmación sonaba a alarmismo de manual. En 2025, ya suena a simple estadística.

Este año ha sido, sin exageración, el más convulso en materia de ciberseguridad que hemos vivido en España. No por un único gran incidente, sino por algo más revelador: la acumulación sistemática de ataques contra objetivos que van desde el Ministerio de Defensa hasta la tarjeta de compra de El Corte Inglés que tienes en el cajón de casa. Lo que ha quedado claro en 2025 es que la amenaza digital ya no distingue entre grandes corporaciones y pequeños negocios, entre adultos expertos y adolescentes conectados desde el salón familiar.

Si sigues creyendo que esto no va contigo, este artículo es exactamente para ti.

El caso que lo resume todo: cuando El Corte Inglés no fue suficiente escudo

En marzo de 2025, uno de los nombres más reconocibles del comercio español se convirtió en protagonista de una brecha de seguridad que afectó potencialmente a los datos de cerca de 11,8 millones de titulares de su tarjeta de compra. Nombres, direcciones, teléfonos y números de tarjeta quedaron expuestos tras un ataque al sistema de un proveedor externo de la compañía.

Este incidente ilustra perfectamente un concepto que los especialistas en ciberseguridad llevamos años explicando: el **ataque a la cadena de suministro**. Los delincuentes no siempre atacan a la gran empresa directamente. Atacan al eslabón más débil de su ecosistema: un proveedor de software, una empresa de logística, una plataforma de marketing. Y a través de ese eslabón, acceden a millones de usuarios que confían en la marca principal.

La lección no es dejar de comprar en grandes superficies. La lección es entender que tu seguridad digital depende, en parte, de decisiones que toman terceros que ni siquiera conoces.

Los números que nadie debería ignorar

Los datos disponibles para 2025 no dejan margen para la complacencia. Según el INCIBE (Instituto Nacional de Ciberseguridad), los incidentes de ciberseguridad en España han crecido un 26% respecto al año anterior, superando los 122.000 casos gestionados. Solo el fraude online ha registrado más de 45.000 incidentes, con el **phishing** —correos o mensajes que suplantan identidades reales para robarte datos— como modalidad dominante con más de 21.000 casos.

Para las empresas, la cifra que más duele es otra: una pyme puede perder entre 2.500 y 60.000 euros tras sufrir un ciberataque. Y lo que resulta verdaderamente alarmante es que el 60% de las pymes que sufren un incidente grave cierran en los seis meses siguientes. No porque el ataque destruya el negocio de forma directa, sino porque la pérdida de datos, de reputación y la interrupción de la actividad se combinan en un golpe del que muchas no logran recuperarse.

¿Qué tiene que ver esto con la familia que lee las noticias en el sofá? Más de lo que parece. Porque detrás de cada pyme atacada hay empleados, autónomos, proveedores y clientes cuyos datos también estaban en esos sistemas.

Ingeniería social: el arma que no necesita tecnología sofisticada

Uno de los aspectos más inquietantes de 2025 es que los ataques más efectivos no han requerido sofisticación técnica. Han requerido psicología. La **ingeniería social** es el arte de manipular a personas para que entreguen información o accedan a sistemas de forma voluntaria, creyendo que hacen lo correcto.

El INCIBE ha documentado casos en los que usuarios mayores han recibido llamadas con la voz clonada de un familiar —generada mediante inteligencia artificial— solicitando dinero de urgencia. No era su familiar. Era una grabación de pocos segundos procesada por una herramienta de IA que cualquier delincuente puede contratar online por menos de lo que cuesta una suscripción de streaming.

Este es el nuevo terreno de juego: los atacantes ya no necesitan romper contraseñas ni vulnerar servidores. Les basta con enviarte un mensaje que parezca de tu banco, llamarte fingiendo ser tu hijo, o hacerse pasar por un técnico de soporte. El factor humano sigue siendo, en 2025, el vector de entrada número uno en la mayoría de los ataques exitosos.

Para las empresas, esto se traduce en empleados que abren archivos adjuntos maliciosos o comparten credenciales ante solicitudes aparentemente urgentes de sus superiores. Para las familias, en abuelos que transfieren dinero, adolescentes que entregan sus contraseñas o padres que instalan aplicaciones fraudulentas creyendo que protegen a sus hijos.

El ransomware ha llegado a tu ayuntamiento

Si hay una amenaza que ha protagonizado los titulares de 2025 en España, es el **ransomware**: un tipo de ataque que secuestra los sistemas informáticos de una organización y exige un rescate económico para liberarlos. Este año, el Ayuntamiento de Badajoz sufrió precisamente esto: sus sistemas quedaron completamente paralizados, afectando a trámites administrativos, portales web y la atención a más de 150.000 ciudadanos.

¿Por qué importa esto a empresarios y familias? Porque si las administraciones públicas, con sus recursos y equipos técnicos, son vulnerables, la pregunta obligada es: ¿cuánto más lo son los negocios medianos, las clínicas locales, los despachos de abogados o los comercios con una única persona gestionando su informática?

España registró un aumento del 116% en ataques de ransomware durante 2025, posicionándose en el top 15 mundial de países más afectados. Detrás de estos ataques no hay hackers solitarios en habitaciones oscuras. Hay organizaciones criminales estructuradas que operan con modelos de negocio propios, subcontratan servicios y se especializan por sectores. Es, literalmente, una industria.

Lo que este año ha cambiado de verdad

2025 no solo ha traído más ataques. Ha traído ataques *cualitativamente* diferentes. La integración de la inteligencia artificial en las herramientas de los atacantes ha elevado el nivel de sofisticación de forma exponencial. Los mensajes de phishing ya no tienen faltas de ortografía. Las llamadas fraudulentas suenan completamente naturales. Los correos maliciosos están personalizados con datos reales obtenidos de filtraciones anteriores.

Esto conecta con otro concepto clave: el **OSINT** (Open Source Intelligence), que en términos sencillos significa la recopilación de información pública sobre una persona o empresa para preparar un ataque dirigido. Todo lo que publicas en redes sociales, la información de tu web corporativa, los perfiles de LinkedIn de tus empleados: es materia prima para quien quiera estudiarte antes de atacarte.

El resultado es una amenaza mucho más personalizada, más creíble y, por tanto, más difícil de detectar con los mecanismos de defensa tradicionales.

Reflexión estratégica: la conciencia como primera línea de defensa

Ante este panorama, sería fácil caer en la parálisis o en el alarmismo. No es lo que pretendo. Lo que quiero transmitir es algo más útil: que la ciberseguridad efectiva no comienza con un software ni con un firewall. Comienza con **comprensión del entorno**.

Un empresario que entiende cómo funciona la ingeniería social es mucho menos vulnerable que uno con el mejor antivirus del mercado pero sin criterio para detectar un correo manipulado. Una familia que habla abiertamente sobre fraudes digitales protege a sus miembros más vulnerables mejor que cualquier control parental.

Los ataques de 2025 han tenido éxito, en su inmensa mayoría, porque las víctimas no esperaban ser objetivo. Creían que eran demasiado pequeños, demasiado anónimos o demasiado poco interesantes para un atacante. Esa percepción es, hoy, el mayor riesgo de todos.

La tecnología ayuda. Las contraseñas robustas, la autenticación en dos pasos, las copias de seguridad periódicas: todo suma. Pero ninguna herramienta técnica sustituye a una cultura digital consciente, tanto en el hogar como en la empresa.

Isaac Ruiz Romero