No todo el que te habla es quien dice ser: suplantación de identidad digital en 2026

Cómo se crea un perfil falso en dos minutos, por qué los menores son el objetivo más fácil y qué hacer cuando algo no encaja.

Aprende qué es la suplantación de identidad digital, cómo detectarla en redes sociales y qué hacer si alguien suplanta tu perfil o el de tu hijo. Guía práctica 2026.

El experimento que nadie debería necesitar hacer

Abre cualquier red social. Crea una cuenta nueva. Sube una foto de alguien atractivo que hayas encontrado en cinco segundos en Google. Añade un nombre común, una ciudad real y dos o tres intereses genéricos: música, viajes, fútbol. Envía solicitudes de amistad a veinte personas. Espera.

En menos de dos minutos tienes un perfil funcional, creíble y listo para engañar. En menos de una hora, probablemente ya tengas entre tres y cinco contactos nuevos que no saben que están hablando con nadie.

Este no es un experimento que yo recomiende hacer. Pero sí uno que explica, mejor que cualquier estadística, por qué la suplantación de identidad digital se ha convertido en uno de los riesgos más silenciosos del ecosistema online actual. No requiere ningún conocimiento técnico. No deja rastro inmediato. Y funciona con una eficacia que resulta incómoda de reconocer.

Qué es exactamente la suplantación de identidad digital

La suplantación de identidad —también conocida en su vertiente anglófona como *catfishing* cuando implica engaño afectivo— es el acto de hacerse pasar por otra persona o crear una identidad falsa para interactuar con terceros con algún tipo de propósito oculto.

Ese propósito puede ser muy variado: obtener información personal, manipular emocionalmente a alguien, extorsionar, ejercer acoso, o en los casos más graves relacionados con menores, iniciar procesos de *grooming*, es decir, el acercamiento gradual y sistemático a un menor con el objetivo de ganar su confianza para después explotarlo sexualmente.

Lo importante es entender que no hablamos de un único tipo de ataque con un único perfil de víctima. La suplantación de identidad afecta a adultos en entornos profesionales —donde un perfil falso de LinkedIn puede ser la puerta de entrada a una operación de espionaje corporativo o ingeniería social— pero también, y de manera especialmente preocupante, a menores en plataformas de mensajería y redes sociales donde la supervisión es mínima y la confianza, máxima.

Caso real: lo que ocurre cuando alguien escribe "hola, ¿nos conocemos?"

En 2024, una chica de catorce años de Valencia recibió una solicitud de seguimiento en Instagram de alguien que decía ser un chico de dieciséis años del instituto de al lado. El perfil tenía fotos, seguidores, publicaciones con meses de antigüedad. Todo parecía normal. Empezaron a hablar. A los pocos días, el perfil le pedía fotos.

Este patrón —y conviene subrayarlo porque se repite con una regularidad perturbadora en los informes de la Agencia Española de Protección de Datos y del Centro de Seguridad en Internet para Menores de España (IS4K)— es el modelo estándar del grooming digital. No empieza con una petición explícita ni con un mensaje amenazante. Empieza exactamente como empieza cualquier amistad online: con normalidad, curiosidad y una conversación que parece inocente.

Los perfiles utilizados en estos casos rara vez son improvisados. Muchos llevan semanas o meses de preparación. Las fotos son robadas de cuentas reales de jóvenes —a menudo de otros países para dificultar la verificación—. El lenguaje que usan imita al de los adolescentes con una precisión que hoy se ve amplificada por herramientas de inteligencia artificial capaces de generar conversaciones enteras que suenan exactamente a cómo habla un chico de dieciséis años.

El caso de Valencia terminó con la intervención de los padres, que habían notado un cambio en el comportamiento de su hija. No todos los casos terminan así.

Por qué los menores son el objetivo más vulnerable

Hay una razón estructural por la que los menores —especialmente los adolescentes de entre doce y dieciséis años— son el segmento más expuesto a este tipo de ataques, y tiene poco que ver con la ingenuidad y mucho con la psicología del desarrollo.

Durante la adolescencia, la necesidad de validación externa, de conexión con iguales y de explorar la propia identidad alcanza su pico más alto. Los adolescentes están biológicamente predispuestos a buscar nuevas relaciones, a abrirse emocionalmente y a confiar en quienes les muestran comprensión. Un adulto que construye un perfil falso de adolescente no está explotando un fallo cognitivo: está explotando una fortaleza humana reconvertida en vulnerabilidad por el contexto digital.

A esto se suma que las plataformas más populares entre jóvenes —TikTok, Instagram, Snapchat, Discord— tienen mecanismos de verificación de identidad prácticamente inexistentes para usuarios nuevos. Cualquiera puede ser cualquiera. Y los menores, en su mayoría, no han recibido formación específica sobre cómo funciona este tipo de amenaza.

El problema adicional es que, cuando el engaño avanza y empieza la fase de manipulación o extorsión, muchos jóvenes no lo cuentan. La vergüenza, el miedo a la reacción de sus padres o la sensación de haber "hecho algo mal" actúa como mecanismo de silencio que beneficia directamente al agresor.

Las señales de alerta que muchos padres no reconocen

No existe una lista cerrada de señales infalibles, pero hay patrones de comportamiento que, en conjunto, merecen una conversación tranquila con tu hijo o hija.

En el comportamiento digital: ocultar la pantalla cuando alguien se acerca, cambiar de aplicación rápidamente, pasar muchas horas al teléfono en momentos inusuales —tarde por la noche, durante las comidas— o mostrar ansiedad cuando el móvil no tiene batería o cobertura.

En el comportamiento general: cambios de humor bruscos relacionados con el uso del teléfono, retraimiento social, pérdida de interés en actividades que antes le gustaban, o referencias a un "amigo" o "amiga" que nadie del entorno conoce en persona.

En las conversaciones: mencionar que alguien le pide que mantenga secretas las conversaciones, que le ha regalado dinero o tarjetas de prepago, o que le pide fotos o información que "es solo para nosotros".

Ninguna de estas señales, tomada de forma aislada, es necesariamente un indicador de que algo está ocurriendo. Pero el patrón conjunto sí lo es, y conviene no descartarlo por la incomodidad que puede generar abrir esa conversación.

Qué hacer si algo no encaja: protocolo práctico

La reacción más contraproducente cuando se detecta que un menor puede estar en contacto con un perfil falso es la confrontación inmediata y el bloqueo sin diálogo. Provoca que el menor cierre el acceso emocional justo cuando más lo necesita.

La primera acción debe ser crear un espacio de conversación sin juicio. No "¿con quién estás hablando?", sino "¿cómo estás? ¿hay algo en el móvil o en las redes que te esté preocupando o haciendo sentir mal?". La diferencia de enfoque cambia completamente la respuesta que obtienes.

Si confirmas que existe un contacto sospechoso, los pasos son concretos. Primero, conservar las evidencias: capturas de pantalla de los mensajes y del perfil antes de bloquear o denunciar. Segundo, denunciar el perfil directamente en la plataforma. Tercero, poner el caso en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado: tanto la Policía Nacional como la Guardia Civil tienen unidades especializadas en delitos tecnológicos y reciben denuncias por canales online. El IS4K (is4k.es), dependiente del INCIBE, ofrece también un servicio de ayuda específico para menores y familias ante incidentes de este tipo.

Si hay intercambio de imágenes comprometidas, la situación es más grave y requiere asesoramiento jurídico especializado. En España existe la posibilidad de solicitar la retirada urgente de contenidos a través de la AEPD, y hay organizaciones como Save the Children con líneas de apoyo específicas para estas situaciones.

La suplantación en entornos profesionales: el otro vector de riesgo

La suplantación de identidad no es solo un problema que afecta a menores. En el entorno profesional, los perfiles falsos en LinkedIn han pasado de ser una curiosidad a convertirse en un vector de ataque activo dentro de las estrategias de ingeniería social más sofisticadas.

Un perfil falso bien construido —con historial laboral plausible, conexiones reales en común y una foto generada por inteligencia artificial que supera cualquier búsqueda inversa de imágenes— puede ser el primer paso de una campaña de *spear phishing* dirigida contra una empresa concreta. El atacante establece contacto, gana confianza, consigue información sobre procesos internos y, cuando tiene suficiente contexto, lanza el golpe: un correo haciéndose pasar por ese contacto, una llamada de seguimiento con datos que solo alguien interno conocería.

La recomendación en este contexto es desarrollar el hábito de verificar por un canal diferente antes de actuar sobre cualquier solicitud que llegue a través de mensajería o correo, especialmente si implica acceso a información sensible, transferencias económicas o cambios en procedimientos habituales. No porque la desconfianza sea la norma, sino porque la verificación cruzada es el único cortafuegos real contra este tipo de ataque.

Reflexión estratégica: el problema no es la tecnología

Hay una tentación natural, cuando se habla de suplantación de identidad digital, de enmarcar el problema como un problema tecnológico con una solución tecnológica. Más filtros, mejores algoritmos de verificación, mayor supervisión de las plataformas. Todo eso ayuda, pero no resuelve el núcleo del problema.

La suplantación de identidad funciona porque la confianza humana no tiene sistema operativo. Confiamos en lo que parece coherente, en lo que encaja con nuestra experiencia previa, en lo que nos hace sentir vistos y comprendidos. Ningún algoritmo puede reemplazar la capacidad crítica que se desarrolla a través de la conversación, la educación y la exposición progresiva a cómo funciona el ecosistema digital real.

En ese sentido, la mejor defensa no es técnica. Es cultural. Es hablar de esto con nuestros hijos antes de que ocurra algo. Es normalizar las conversaciones sobre qué les genera malestar en internet. Es construir el tipo de relación en la que un menor sabe que puede contar algo comprometedor sin que la primera reacción sea la reprimenda.

Y es también, para los adultos, desarrollar el hábito de la fricción consciente: ese segundo de pausa antes de hacer clic, antes de compartir, antes de aceptar una solicitud de alguien que no conocemos en persona, en el que nos preguntamos si lo que estamos viendo es lo que parece ser.

Tu próximo paso

Si este artículo te ha resultado útil, hay tres cosas que puedes hacer hoy: hablar con tu hijo o hija sobre qué hace cuando alguien desconocido le escribe en redes sociales, revisar la configuración de privacidad de sus perfiles para limitar quién puede enviarle mensajes, y guardar el número del IS4K (017) como referencia para cualquier incidente de este tipo.

No necesitas ser experto en tecnología para proteger a quien quieres. Necesitas estar informado, estar presente y tener la conversación antes de que sea necesaria.

Si este artículo te ha ayudado, compártelo con otros padres o educadores. Una comunidad informada es la mejor red de protección que existe. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero.