Un *hacker* aparentemente obtuvo acceso al monitor para bebés de una niña de dos años, la llamaba por su nombre y la acosaba con insultos, al igual que a sus padres.

Una pareja de Houston, Texas, dijo el pasado fin de semana a la filial de CNN, KTRK, que escucharon una voz extraña en la habitación que comparten sus dos hijos. Marc Gilbert dijo al entrar en la recámara notaron que la voz venía del monitor con cámara web que utilizan para vigilar a los niños.

Lo que escucharon después fue terrible.

“Dijo: ‘Despiértate Allyson, pequeña golfa’”, afirmó Gilbert. Dijo que el *hacker*, quien tenía un acento británico o europeo, pudo haber leído el nombre de la niña en un letrero grande colgado en la pared, sobre la cabecera de la cama de la pequeña.

Gilbert dijo que cuando él y su esposa Lauren entraron, la cámara giró hacia su dirección para mirarlos de frente. Antes de que desconectaran la cámara, el *hacker* lo llamó “estúpido idiota” y a su esposa una «perra», dijo Gilbert.

Lo único positivo de la situación fue que Allyson nunca se despertó, dijo. Nació con sordera y usa implantes cocleares para oír, los cuales no traía puestos mientras dormía.

“Me sentí como si alguien se hubiera metido a nuestra casa”, dijo Gilbert. “Como padre, es mi deber protegerla de gente como esta. Así que es un poco vergonzoso, por decir lo menos, pero no ocurrirá de nuevo”.

En el pasado, se ha demostrado la vulnerabilidad de los monitores para bebés, particularmente los que tienen video.

Los monitores con cámara pueden transmitir la señal a televisores, receptores de mano, computadoras, *smartphones* y tabletas.

En 2009, una familia de Illinois, Estados Unidos, demandó al fabricante de su monitor después de descubrir que ellos y sus vecinos podían monitorear las transmisiones del resto.

Algunos modelos más nuevos tienen la tecnología que alterna entre varias frecuencias, lo que los hace más seguros.

Los expertos en seguridad recomiendan a los padres asegurarse de activar contraseñas en los monitores para bebés y las cámaras web. Esto se puede hacer en la mayoría de los modelos nuevos.

“Los dispositivos pueden protegerse con contraseñas, pero las contraseñas de origen que no se cambiaron son como no tener ninguna contraseña”, escribió Lisa Vaas para el blog Sophos Security.

Los expertos también recomiendan asegurarse de que los enrutadores y el *wi-fi* de casa estén protegidos con clave de acceso.

“Quienes no puedan descifrar esto, deben pedir ayuda a alguien con experiencia en seguridad; alguien a quien confíen la seguridad de cosas extremadamente valiosas”, dijo Vaas.

Marc Gilbert dijo que tomó las precauciones básicas de seguridad: “El enrutador estaba protegido con una contraseña y el *firewall* estaba habilitado. La cámara IP también estaba protegida con contraseña”.

“Por supuesto, los dispositivos pueden estar protegidos por contraseñas, pero las contraseñas por defecto que no se cambiaron son como no tener ninguna contraseña, como otros lectores señalaron”, escribió Vaas en el blog Sophos Security.

Fuente: CNN