

اختراق السيارات عن بُعد.. تحذيرات من تهديدات إلكترونية جديدة



يحدّر محللون من تزايد المخاطر الإلكترونية على السيارات الحديثة مع الاعتماد المتصاعد على أنظمة القيادة الذاتية والاتصال الرقمي، ما قد يتيح للقراصنة التحكم بوظائف المركبة والاطلاع على بيانات شخصية، في حين تشدد الشركات المتخصصة على ضرورة تعزيز أنظمة الحماية لضمان سلامة السائقين والمستخدمين.

وبحسب ما نقلته وكالة الأنباء الألمانية عن شركة BMI البريطانية التابعة لمجموعة فيتك سيليوشنز للخدمات المالية، فإن احتمالات الهجمات الإلكترونية على السيارات ستزايد مع تعاظم دور البرمجيات في تشغيل المركبات وارتفاع الاعتماد على أنظمة القيادة الذاتية.

ويؤكد المحللون أن «التسارع المستمر نحو مركبات تعتمد كلياً على البرمجيات» ودمجها في البنية الرقمية الواسعة لشبكات الاتصالات والمعلومات سيضاعف من حجم التهديدات، رغم الفوائد المفترضة لهذه التكنولوجيا، مثل الخرائط المتقدمة والتحديثات اللاسلكية، وتحسين كفاءة الأداء وتجربة القيادة.

وتشير BMI إلى أن السيارات المتصلة بالانترنت باتت معرضة للاختراق مثلها مثل أي جهاز يعمل عبر الشبكة، كاشفة أن باحثين نجحوا بالفعل في اختراق طرز من سوبارو وكيا باستخدام رقم لوحة السيارة فقط، ما أتاح لهم التحكم عن بُعد في وظائف رئيسية، والاطلاع على سجلات المواقع وبيانات الاتصال الشخصية.

وتحذر الشركة من أن هذه التهديدات لا تمس الخصوصية فحسب، بل قد تمتد لتطال «وظائف السيارة الحيوية»، بما يفتح المجال لـ«سيناريوهات خطيرة» كتوجيه المركبة عن بُعد أو السيطرة عليها بالكامل.

ويشدد الباحثون على أن الكرة الآن في ملعب شركات صناعة السيارات، التي باتت مطالبة بتطوير أنظمة حماية أكثر صرامة؛ لمنع عمليات القرصنة وضمان سلامة السائقين والمستخدمين.