TPM 2.0

คือ อะไร

ทำไมถึงเป็นสิ่งจำเป็นสำหรับ WINDOWS 11

หลังจาก Windows 11 เปิดตัวขึ้น ทาง Microsoft ก็ได้ประกาศว่า เวอร์ชั่นนี้ ควรจะใช้งานร่วมกับ คอมพิวเตอร์ ที่มีชิป Trusted Platform Module (TPM) 2.0 ซึ่ง ทำให้หลายๆ คน อาจจะสงสัย ว่า มัน คือ อะไร บทความนี้ เราจะมา อธิบายให้ทราบกันโดยละเอียด

ระบบปฏิบัติการ Microsoft Windows 11 ตัวใหม่ล่าสุดนี้ จำเป็นต้องทำงานร่วมกับชิป TPM เพื่อให้ฟีเจอร์ความปลอดภัยด้าน Security ต่างๆ สามารถทำงานได้อย่างมีประสิทธิภาพมากที่สุด ซึ่งคอมพิวเตอร์ส่วนใหญ่ โดยเฉพาะรุ่นฝั่งโมเดล Commercial นั้น มักจะมาพร้อมชิปชนิดนี้อยู่แล้ว แต่สำหรับเครื่องเก่าๆ หรือรุ่น Consumer ต้องตรวจสอบเป็นรายโมเดลไปครับ บทความนี้เราจะสอนวิธีการเช็คและตรวจสอบเช่นกัน

TPM 2.0 คือ อะไร

โดยพื้นฐานทั่วไป TPM 2.0 คือ ชิปขนาดเล็ก ที่ติดตั้งอยู่บนเมนบอร์ด หรือ Motherboard ของคอมพิวเตอร์ โดยมากจะแยกออกมาจาก CPU และ Memory โดยถ้าเปรียบ PC ของคุณเป็นบ้านหลังหนึ่ง Chip ชนิดนี้ ก็เปลี่ยนเสมือนระบบกันขโมยที่สามารถแจ้งเตือนได้เมื่อมีสิ่งอันตรายบุกรุก

ถ้าคุณกดเปิดปุ่ม Power ของ PC เครื่องใหม่ ที่มีระบบ Encryption และชิป TPM ติดตั้งมาอยู่แล้ว ตัวชิปเอง จะทำการจัดหา Code พิเศษที่ไม่ซ้ำใคร ขึ้นมาสำหรับอุปกรณ์ เรียกว่า Cryptographic Key ถ้าระบบทุกอย่างของตัวเครื่องทำงานได้อย่างปกติดี Drive Encryption นี้จะทำการปลดล็อค ทำให้เครื่องของคุณ Start Up ได้ปกติ แต่หากมีความผิดปกติเกิดขึ้นกับ Key ตัว PC จะไม่ทำการ Boot Up ให้ใช้งาน เช่น มี Hacker ขโมย Laptop ของคุณไป และพยายาม Login ด้วยโปรแกรม Encrypted เจ้าชิปทีพีเอ็มนี้ ก็จะดำเนินการ Lock ไม่ให้ตัวเครื่องทำงานได้ปกติ เป็นต้น

ตัวอย่าง Application ที่มีการทำงานร่วมกับชิป TPM

- Thunderbird และ Outlook Email ใช้ชิปทีพีเอ็มในการ Encrypted หรือ Key-Signed Message
- Firefox และ Google Chrome ใช้ชิป TPM ในการบริหารจัดการ SSL Cerificates สำหรับ Website
- อุปกรณ์ Consumer ต่างๆ นอกจาก PC ก็มีการใช้ชิปทีพีเอ็มเช่นกัน ตั้งแต่ Printer ไปจนถึงอุปกรณ์ไอทีอื่นๆ

นอกจากฟังก์ชั่นความปลอดภัย ที่ตัวมันเองทำได้หลากหลาย เหนือกว่าแค่ Boot-Up ตัวเครื่องอย่างปลอดภัยแล้ว ลักษณะทางกายภาพของตัว TPM 2.0 เอง ก็ไม่ได้มีแต่ลักษณะ Chip แบบ Standalone เช่นกัน โดยทาง Trusted Computing Group (TCG) ซึ่งเป็นองค์กรที่คอยควบคุมมาตรฐาน TPM ได้มีการพัฒนา ทีพีเอ็ม ที่สามารถติดตั้งประกอบเข้ากับ CPU หลัก ทั้งแบบกายภาพโดยตรง หรือเป็น Code ซ่อนอยู่แบบ Firmware อีกด้วย ซึ่งผลลัพธ์ก็ คือ ประหยัดเนื้อที่เมนบอร์ดมากขึ้น แต่สามารถทำงานได้อย่างเต็มประสิทธิภาพเหมือนเดิม

และสุดท้ายนี้ ยังมี TPM อีกชนิดที่มีการพัฒนาขึ้นมา แต่ยังไม่เป็นที่นิยมมากนัก ได้แก่รูปแบบ Virtual ที่ทำงานใน Software ทั้งหมด ซึ่งไม่ค่อยเป็นที่แนะนำเท่าไหร่ เพราะยังใหม่ และมีบัคอยู่พอสมควร

ผู้เขียนบทความนายจรินทร์เดช จำรัสภูมิ
ตำแหน่งช่างเครื่องคอมพิวเตอร์

เรียนรู้เพิ่มเติมที่
https://cc.msu.ac.th/th/cms