ป้องกันอย่างไรไม่ให้ข้างบ้านมาใช้ไวร์เลสบ้านเรา

ระบบความปลอดภัยเป็นเรื่องสำคัญสำหรับระบบเครือข่ายไร้สาย เปรียบเสมือนบ้านที่ต้องการกลอนประตู เพื่อป้องกันผู้บุกรุก กลอนประตูก็มีให้เลือกหลายแบบให้เลือกใช้ได้ตามความจำเป็น กลอนประตูบางชนิดอาจป้องกันได้เฉพาะผู้ที่มาเยี่ยม ไม่ให้เข้าบ้านได้ก่อนที่เจ้าของบ้านจะอนุญาต แต่ไม่สามารถป้องกันขโมยที่มุ่งประสงค์จะงัดแงะ เพื่อเข้ามาขโมยของในบ้านเราไปจนได้ การป้องกันขโมยมืออาชีพจึงอาจมีความจำเป็นต้องเพิ่มระบบกันขโมยที่แน่นหนา เฉพาะกิจมากกว่าแค่กลอนประตู การสร้างความปลอดภัยในระบบเครือข่ายไร้สายก็มีหลากหลายเช่นกัน ขึ้นอยู่กับความจำเป็นในการใช้งาน ความสำคัญของข้อมูล ความเสี่ยงในการที่บุคคลภายนอกจะสามารถแอบเข้ามาร่วมใช้งานในระบบของเรา

โดยทั่วไประบบเครือข่ายในองค์กรขนาดกลางถึงใหญ่มักจะมีความจำเป็นอย่างยิ่งที่จะต้องใช้วิธีการจัดการด้านความปลอดภัยที่แน่นหนา รัดกุม แต่สำหรับระบบเครือข่ายไร้สายภายในบ้าน หรือออฟฟิตขนาดเล็ก ยังมีวิธีการง่ายๆ เป็นการสร้างความปลอดภัยเบื้องต้นที่สามารถป้องกันไม่ให้ผู้อื่นเข้ามาแอบดึงข้อมูลไปจากระบบเครือข่ายของเราได้ หรือแม้แต่เข้ามาใช้งานในเครือข่ายของเรา บทความฉบับนี้จึงเป็นการนำเสนอการรักษาความปลอดภัยแบบง่ายๆให้กับท่าน พึงระลึกว่าบางวิธีการอาจไม่สามารถป้องกันได้แน่นหนานัก แฮกเกอร์มืออาชีพยังสามารถเจาะเข้าไปในระบบได้โดยไม่ยาก แต่นั่นก็หมายความว่าต้องเป็นผู้ที่มีความรู้ทางด้านเทคนิคพอสมควร มิใช่เพียงข้างบ้านทั่วๆไปเท่านั้น

10 วิธีง่ายๆ ในการสร้างระบบรักษาความปลอดภัยให้ไวร์เลสเน็ตเวิร์คที่บ้าน

1. No Default Settings
2. Cell Sizing
3. SSID Naming
4. Cloaking
5. MAC Filters
6. Encryption
7. Static IP
8. Common Security Practices
9. Document Your Settings
10. Turn it off

No Default Settings
สิ่งที่คนจำนวนมากพลาด คือการไม่ได้เข้าไปเปลี่ยนชื่อบางชื่อให้กับอุปกรณ์แม่ข่ายของระบบ อาทิ โมเด็ม เร้าเตอร์ และแอ็คเซสพอยส์ โดยปกติอุปกรณ์เหล่านี้จะมีการตั้งชื่อมาจากโรงงาน ตามแต่ละยี่ห้อจะตั้ง ชื่อและรหัสผ่านเหล่านั้นจะแสดงอยู่ในคู่มือการติดตั้งอุปกรณ์ ดังนั้นหากคนที่ต้องการจะเข้ามาใช้อินเตอร์เน็ตหรือใช้งานในระบบของเราทราบว่าเราใช้อุปกรณ์รุ่นใด ก็สามารถดาว์นโหลดคู่มืออินเตอร์เน็ต และเพิ่มตัวเองเข้าไปในระบบได้โดยง่าย

ค่าหรือชื่อที่ท่านควรเข้าตั้งค่าใหม่
- SSID (Service Set Identifier)
- The administrator login Name (User Name) / Password

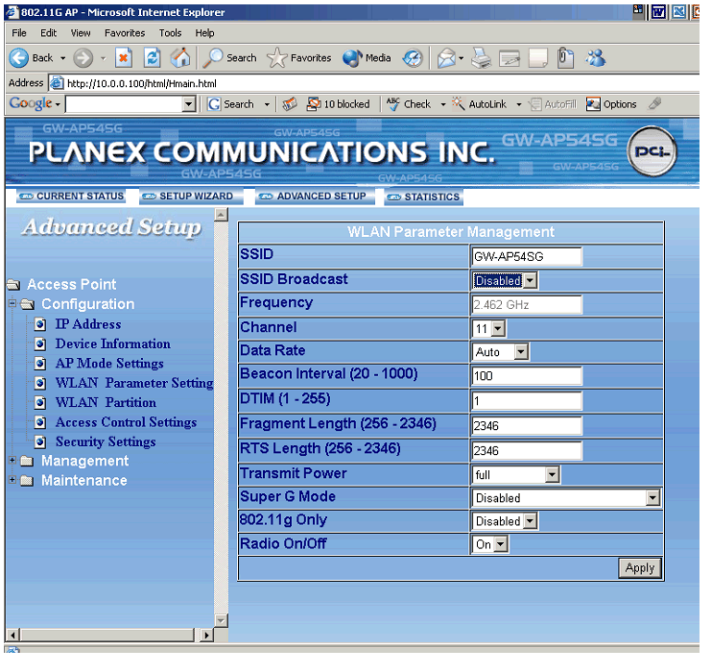
การเข้าไปเปลี่ยนชื่อ SSID ทำได้โดย การเข้าไปที่หน้าคอนฟิคของสินค้า → Advanced Set Up → WLAN Parameter Setting → ตั้งชื่อ SSID ตามที่ท่านต้องการ

Cell Sizing

ความเชื่อที่ว่ายิ่งแรงยิ่งดี มักมาคู่กับการที่ท่านแบ่งสัญญาณเครือข่ายไร้สายให้ข้างบ้านใช้งานด้วย ดังนั้นในการติดตั้งระบบเครือข่ายไร้สายควรดูรัศมีที่ท่านต้องการจะใช้งาน และเลือกใช้ และติดตั้งอุปกรณ์ที่ส่งสัญญาณได้เหมาะสมกับรัศมีนั้น

- ในปัจจุบันสินค้าบางรุ่นจะมีคุณสมบัติที่เรียกว่า "Adjust antenna transmit power" ให้ท่านสามารถปรับให้กำลังส่งลดลงได้
- หรือหากอุปกรณ์ที่ท่านใช้อยู่นั้นไม่สามารถปรับค่ากำลังส่งได้ ท่านสามารถติดตั้งอุปกรณ์ให้อยู่กลางบ้าน หลีกเลี่ยงการวางใกล้หน้าต่าง

การเข้าไป Adjust antenna transmit power ทำได้โดย การเข้าไปที่หน้าคอนฟิคของสินค้า → Advanced Set Up → WLAN Parameter Setting → เลือกระดับของ Transmit Power



SSID Naming

จากที่กล่าวข้างต้น ว่าท่านควรเปลี่ยนชื่อ SSID ให้ต่างจากชื่อที่มาจากโรงงาน ชื่อที่ตั้งใหม่ก็ควรหลีกเลี่ยงชื่อที่ใกล้ตัวท่านมากเกินไป อาทิ ชื่อจริง ชื่อเล่น นามสกุล ชื่อบริษัท ควรเป็นชื่อที่ไม่มีความหมาย หรือยากแก่การคาดเดา เพราะบุคคลที่ต้องการเข้ามาในระบบของท่านอาจลองเสี่ยงใช้เพื่อเข้าระบบของท่านได

Cloaking

อุปกรณ์กระจายสัญญาณ อาทิ Access Point จะมีการตั้งค่าหนึ่งเรียกว่า "Closed Network" หรือ "Broadcast SSID" การที่ท่านปิดเน็ตเวิร์ค (enabling Closed Network) หรือ ตั้งค่าไม่ให้เผยแพร่ SSID (disabling Broadcast SSID) จึงเป็นเสมือนการซ่อนไม่ให้อุปกรณ์ลูกข่ายสามารถหา Access Point เจอ และไม่สามารถเข้ามาในระบบได้

ในการทำงาน Access Point จะส่งแพ็คเก็ตเล็กๆออกมา กระจายไปในอากาศ ด้วยอัตราการส่งจำนวนหนึ่ง อาทิ 100 แพ็คเก็ตต่อวินาที เรียกว่า Beacon (บีค่อน) ในบีค่อนจะมีข้อมูลต่างๆ รวมทั้ง SSID (Network Name) อยู่ด้วย ในตลาดจะมีอุปกรณ์ตัวหนึ่งเรียกว่า Network Stumbler ใช้สำหรับสแกนหา Access Point โดยการส่ง "Blank Probe Request" ออกไปในอากาศ หากท่านตั้งค่า disabling Broadcast SSID ที่ Access Point ของท่าน บีค่อนที่ Access Point ส่งออกมาจะไม่ปรากฏชื่อ SSID และไม่สามารถตอบรับกับ blank Probe Request ได้ ทำให้ Network Stumbler ไม่สามารถหา Access point เจอ กล่าวได้ว่าเป็นการสร้างความปลอดภัยให้กับระบบเครือข่ายของท่านได้

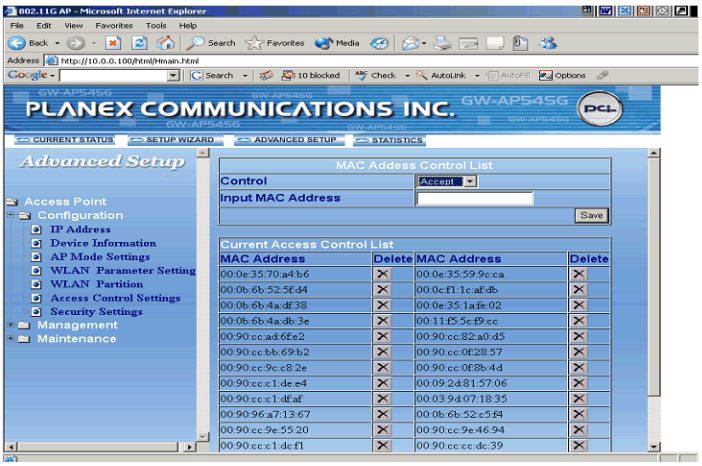
อย่างไรก็ตาม พึงระลึกว่าวิธีนี้เป็นการสร้างความปลอดภัยได้ระดับหนึ่งเท่านั้น แฮ็กเกอร์มืออาชีพยังคงมีหลากหลายวิธีที่สามารถหาชื่อ SSID ของท่านได้

การเข้าไป Disabling Broadcast SSID ทำได้โดย การเข้าไปที่หน้าคอนฟิคของสินค้า → Advanced Set Up → WLAN Parameter Setting → เลือก Disable Broadcast SSID

MAC Filters

ที่ด้านหลังของไวร์เลสอแดปเตอร์ จะมีข้อมูลหนึ่งเป็นการผสมระหว่างตัวเลขกับตัวอักษร จำนวน 12 หลัก เรียกว่า "MAC address" (พลิกดูด้านหลังอแดปเตอร์ มองหา MAC address หรือบางอแดปเตอร์จะใช้ชื่อเรียกว่า Node ID) ในขณะที่เร้าเตอร์ แอ็คเซสพอยส์จะมีการตั้งค่าหนึ่งที่ให้ท่านสามารถกรอกรายชื่อ MAC address ที่ท่านยอมให้เข้ามาใช้งานในระบบได้ ซึ่งหมายความว่า หากท่านกรอกรายการเฉพาะ MAC addresses ของการ์ดที่ท่านและคนในบ้านใช้งาน ก็จะป้องกันไม่ให้การ์ดของเพื่อนบ้าน ซึ่งไม่ได้อยู่ในรายการเข้ามาใช้งานในระบบได้

การเข้าไประบุรายชื่อ MAC address ทำได้โดย การเข้าไปที่หน้าคอนฟิคของ Access Point → Advanced Set Up → Access Control Setting → (1) เลือก Accept ที่ Control (2) ระบุ MAC address ที่ต้องการ → กด save



Encryption

พึงระลึกเสมอว่าการทำงานของระบบเครือข่ายไร้สาย เป็นการรับส่งข้อมูลในอากาศ นั่นก็หมายความว่าถ้ามีใครสามารถจับข้อมูลที่เราส่งออกไปในอากาศนั้นได้ ก็สามารถอ่านข้อมูลของเราได้ แอบอ่านอีเมล์ หรือขโมย User Name / Password เราได้เช่น การเข้ารหัสข้อมูล (Encryption)

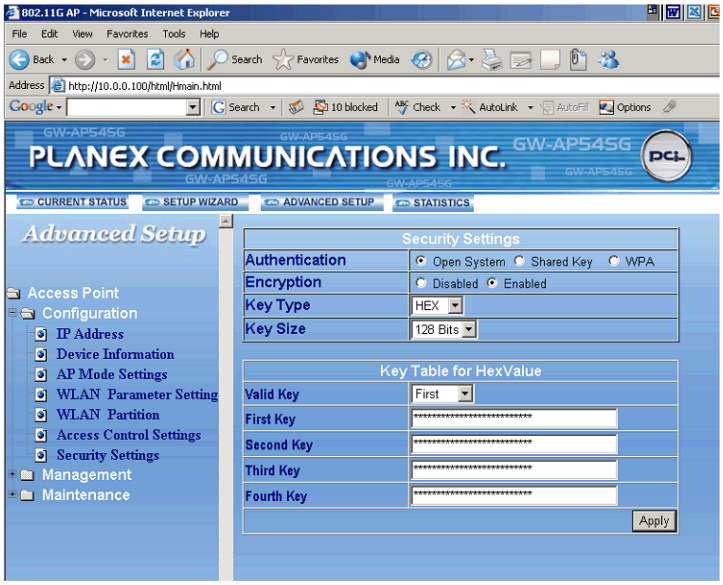
ตามมาตรฐานจากโรงงาน อุปกรณ์ไร้สายจะรองรับเทคโนโลยีการเข้ารหัส ซึ่งมีหลากหลายเทคโนโลยี

- WEP (Wired Equivalent Privacy)
- TKIP (Temporal Key Integrity Protocol) เป็นเวอร์ชั่นที่พัฒนามาจาก WEP
- AES (Advanced Encryption Standard)

ถ้าอุปกรณ์ที่ท่านใช้อยู่รองรับ WEP ให้เข้าไป enable WEP ของทั้งที่ Access Point และ อแดปเตอร์ จะเป็นการทำให้ทุกข้อมูลที่รับส่งในอากาศมีการเข้ารหัส ทำให้อุปกรณ์ที่ไม่ได้มีการเข้ารหัสร่วมกับเราไม่สามารถรับและแปลงรหัสนั้นได้ ดังนั้นในการตั้งรหัส ท่านจะต้องตั้งรหัสทุกอุปกรณ์ให้ตรงกัน ไม่เช่นนั้นจะเป็นการล็อคตัวท่านเองให้ไม่สามารถอ่านข้อมูลนั้นได้ด้วย อย่างไรก็ตาม WEP เป็นการรักษาความปลอดภัยอย่างง่าย ซึ่งปัจจุบันการปลดรหัส WEP ทำได้ง่ายมาก แฮกเกอร์สามารถปลดรหัสได้ภายใน 5นาที

การเข้าไประบุรายชื่อ MAC address ทำได้โดย การเข้าไปที่หน้าคอนฟิคของ Access Point → Advanced Set Up → Security Setting → (1) เลือก Open System ที่ Authentication (2) เลือก Enabled ที่ Encryption (3) เลือก HEX หรือ ASCII ที่ Key Type (4) เลือก 152, 128 หรือ 64 bits ที่ Key Size (5) กรอกรหัสที่ต้องการตั้งในช่อง First Key (ต้องเป็นรหัสเดียวกันกับที่ใช้ในการตั้งค่าที่อแดปเตอร์ทุกตัวที่จะใช้ในระบบ) การตั้งค่ารหัสจะมีหลักการที่แตกต่างกันไป ตามแต่ Key Type และ Key Size ที่เลือก

Key Type	Key Size	First Key
HEX	152 bits	ผสมตัวเลข ตัวอักษรให้ได้ 32 หลัก จากเลข 0-9 และอักษร A – F (ตัวอักษรใหญ่เล็กไม่มีผล)
HEX	128 bits	ผสมตัวเลข ตัวอักษรให้ได้ 26 หลัก จากเลข 0-9 และอักษร A – F (ตัวอักษรใหญ่เล็กไม่มีผล)
HEX	64 bits	ผสมตัวเลข ตัวอักษรให้ได้ 10 หลัก จากเลข 0-9 และอักษร A – F (ตัวอักษรใหญ่เล็กไม่มีผล)
ASCII	152 bits	ผสมตัวเลข ตัวอักษรให้ได้ 16 หลัก จากเลข 0-9 และอักษร A – Z (ตัวอักษรใหญ่เล็กไม่มีผลต่อการตั้งรหัส ส่วนเครื่องหมายพิเศษจะใช้ได้หรือไม่ขึ้นอยู่กับ firmware ของรุ่นนั้นๆ)
ASCII	128 bits	ผสมตัวเลข ตัวอักษรให้ได้ 13 หลัก จากเลข 0-9 และอักษร A – Z (ตัวอักษรใหญ่เล็กไม่มีผลต่อการตั้งรหัส ส่วนเครื่องหมายพิเศษจะใช้ได้หรือไม่ขึ้นอยู่กับ firmware ของรุ่นนั้นๆ)
ASCII	64 bits	ผสมตัวเลข ตัวอักษรให้ได้ 5 หลัก จากเลข 0-9 และอักษร A – Z (ตัวอักษรใหญ่เล็กไม่มีผลต่อการตั้งรหัส ส่วนเครื่องหมายพิเศษจะใช้ได้หรือไม่ขึ้นอยู่กับ firmware ของรุ่นนั้นๆ)



หากผลิตภัณฑ์ที่ท่านใช้ได้รับการรับรอง WPA (WiFi Protected Access Certified) อุปกรณ์นั้นจะรองรับการเข้ารหัส TKIP ซึ่งจะใช้หลักการเดียวกับการเข้ารหัส WEP คือทั้ง Access Point และ อแดปเตอร์ที่ท่านใช้จะต้องมี WPA Certified.

การเข้ารหัส TKIP ให้ไปที่ security setting แล้วเลือก WPA-Pre-Shared Key (หรือบางครั้งอาจใช้ชื่อ WPA Passphrase)

ทั้งนี้ผลิตภัณฑ์เก่าที่สนับสนุนแต่เพียง WEP อาจจะมีเฟิร์มแวร์ (firmware) ที่สามารถอัพเกรด WPA ได้ จึงขอแนะนำให้ท่านเข้าไปตรวจสอบในเวบไซต์แบรนด์ผลิตภัณฑ์ที่ท่านใช้ ดูว่าท่านสามารถอัพเกรด WPA / TKIP ได้หรือไม่

หากผลิตภัณฑ์ที่ท่านใช้ได้รับการรับรอง WPA2 (WiFi Protected Access – version 2) หมายความว่าอุปกรณ์ไร้สายที่ท่านใช้สนับสนุน AES การเข้ารหัส AES จะต้องเข้าตั้งค่าทั้งที่ Access Point และ อแดปเตอร์เช่นเดียวกับการเข้ารหัสอื่นๆที่กล่าวมาแล้ว

การเข้ารหัส AES ให้ไปที่ security setting แล้วเลือก WPA2-Pre-Shared Key (หรือบางครั้งอาจใช้ชื่อ WPA2 Passphrase)

ผลิตภัณฑ์รุ่นเก่าๆโดยทั่วไปจะไม่สามารถอัพเกรดเฟิร์มแวร์เพื่อการเข้ารหัส AES ได้ อย่างไรก็ตามควรติดต่อหรือเข้าไปที่เว็บไซต์ของแบรนด์ผลิตภัณฑ์ที่ท่านใช้เพื่อตรวจสอบอีกครั้ง

Static IP

เร้าเตอร์ที่มีฟังก์ชั่น DHCP จะทำการแจก IP address ให้กับอแดปเตอร์ โดยการแจกจะไม่ใช่เลข IP ที่คงที่ แต่จะเปลี่ยนไปเรื่อยๆ ตามการใช้งานแต่ละครั้ง ซึ่งอาจเป็นไปได้ว่าจะไปแจกให้กับเครื่องของคนอื่นที่ต้องการเข้ามาใช้งานในระบบได้เหมือนกัน

ลองพิจารณาการใช้วิธีการแจก IP address แบบคงที่ โดยการ disabling DHCP setting ที่เร้าเตอร์ แล้วให้ท่านเลือกเลขที่ IP ให้กับอแดปเตอร์ทุกตัวของท่านด้วยตัวท่านเอง ซึ่งอาจจะดูไม่สะดวกแต่จะเป็นการสร้างความปลอดภัยให้กับระบบไร้สายของท่านได้มากกว่า

ท่านสามารถ Disable DHCP ที่ Access Point หรือเร้าเตอร์ โดยการ เข้าไปที่หน้า Configuration → เลือก LAN → เลือก Disabled ที่ DHCP Server

แล้วเข้าไปตั้งค่า IP ที่ท่านต้องการ (manually) ให้อแดปเตอร์จากหน้าจอคอมพิวเตอร์ โดยการกด Start → Setting → Network Connection → Wireless Network Connection → จะขึ้นหน้าต่าง Wireless Network Connection Status ให้เลือก Properties → Double Click ที่ Internet Protocol (TCP/IP) → จะขึ้นหน้าต่าง Internet Protocol (TCP/IP) Properties →เลือก Use the following IP address จากนั้นกรอกค่า IP ที่ต้องการ โดยจะต้องสอดคล้องกับ ค่า Default gateway (ค่า IP ของ Router หรือ Access Point ที่ใช้) คือกำหนดให้ตัวเลข 3 ชุดแรกเหมือนกัน แต่ชุดที่ 4 ต้องไม่เหมือนกัน (ตามที่แสดงในตาราง)

	Class A	Class B	Class C
IP address ที่ต้องการ	10.0.0.y	172.16.7.y	192.168.0.y
Subnet	255.0.0.0	255.255.0.0	255.255.255.0
Default gateway	10.0.0.x	172.16.7.x	192.168.0.x

โดยค่า y ที่ท่านกำหนดจะต้องไม่เท่ากับ x

Common Security Practices

เลือกการใช้งานข้อปฏิบัติบางอย่างที่เหมาะสม อาทิ

- ติดตั้งโปรแกรมป้องกันไวรัส ดาว์นโหลด virus signatures files- ไฟล์ที่รวบรวมชื่อและลักษณะของไวรัสประเภทต่างๆไว้ และจะตรวจจับเมื่อไวรัสลักษณะนั้นเข้ามาในระบบ ไม่ให้สามารถเข้าสู่ระบบได้โดยง่าย
- หากไม่มีความต้องการใช้ไฟล์งานร่วมกันระหว่างเครื่อง ควร disable file sharing
- ลองพิจารณาติดตั้ง Personal firewalls ให้กับทุกๆเครื่องคอมพิวเตอร์

Document Your Settings

จากคำแนะนำต่างๆข้างต้น มีหลายข้อมูลที่ท่านต้องมีการตั้งชื่อใหม่ หรือตั้งค่าใหม่ ในครั้งนี้จึงขอแนะนำให้ท่านจดค่าต่างๆเหล่านั้นในที่ที่ปลอดภัย เผื่อกรณีที่ท่านจำเป็นต้อง reset อุปกรณ์ต่างๆ ซึ่งท่านจำเป็นต้องกลับไปที่ค่าที่ตั้งมาจากโรงงาน default settings) และต้องเริ่มต้นใหม่อีกครั้ง

Turn it off

คำแนะนำสุดท้ายคือการปิดเครื่องในขณะที่ท่านไม่ได้ใช้งาน เพราะคนอื่นจะไม่สามารถเข้ามาใช้งานในระบบของท่านได้ หากท่านปิดเครื่องนั้นเสีย

ที่มา: www.globalknowledge.com

หมายเหตุ: สินค้าแต่ละแบรนด์ แต่ละรุ่น อาจมีวิธีการเรียกชื่อการตั้งค่าต่างกัน ทั้งนี้บทความนี้แสดงลำดับวิธีการตั้งค่าจาก สินค้า PCi รุ่น GW-AP54SG และสินค้า Tactio รุ่น ALTERA-04G สำหรับสินค้ารุ่นอื่นๆ ท่านสามารถศึกษาได้จากคู่มือการติดตั้ง หรือติดต่อบริษัทผู้ผลิตเพื่อสอบถามข้อมูลเพิ่มเติม