การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ให้มีความปลอดภัย

1.Antivirus / Windows Defender

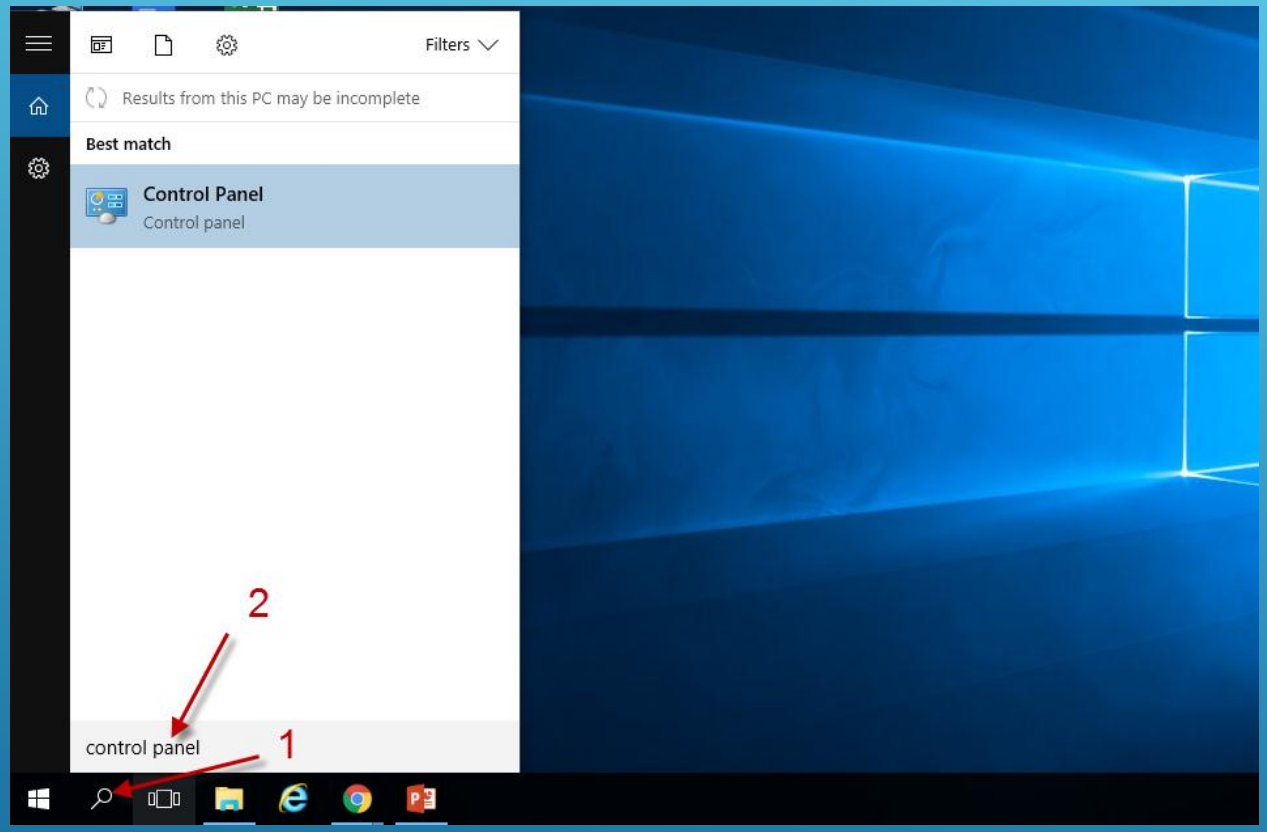
2. Windows Firewall

3. การตั้งค่า Access Point เพื่อใช้งานในมหาวิทยาลัย

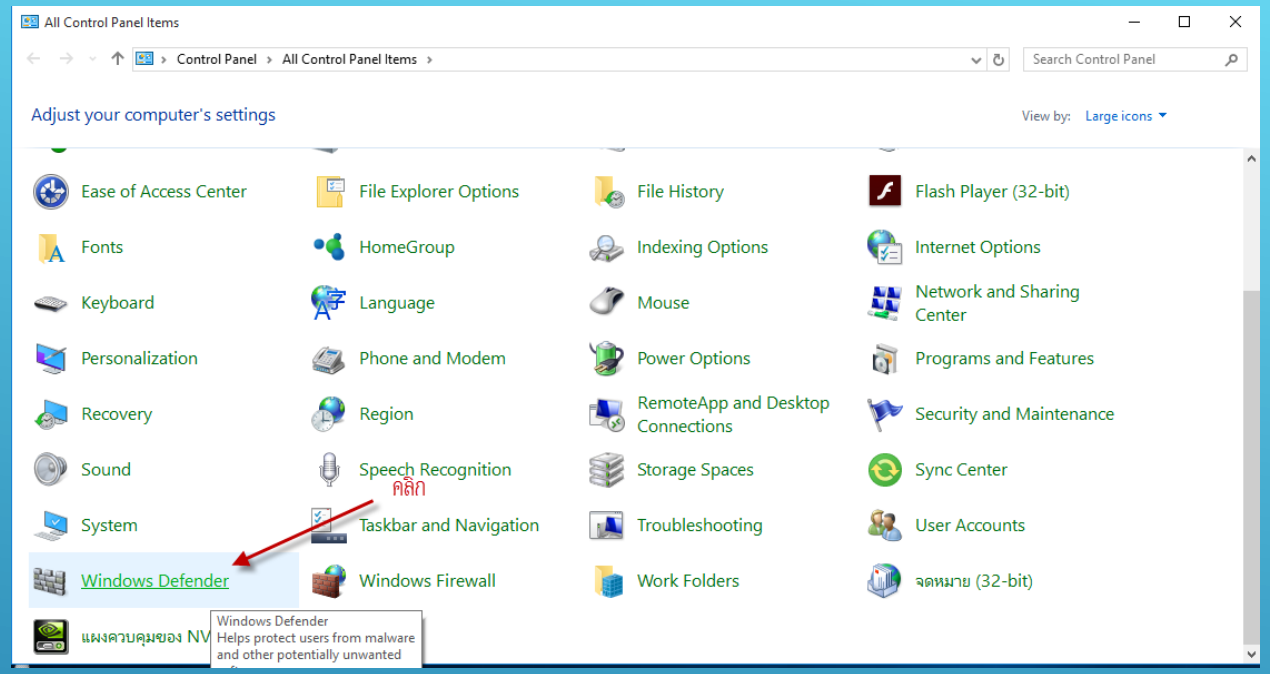
4. การค้นหาช่องสัญญาณเพื่อใช้งานให้มีประสิทธิภาพ

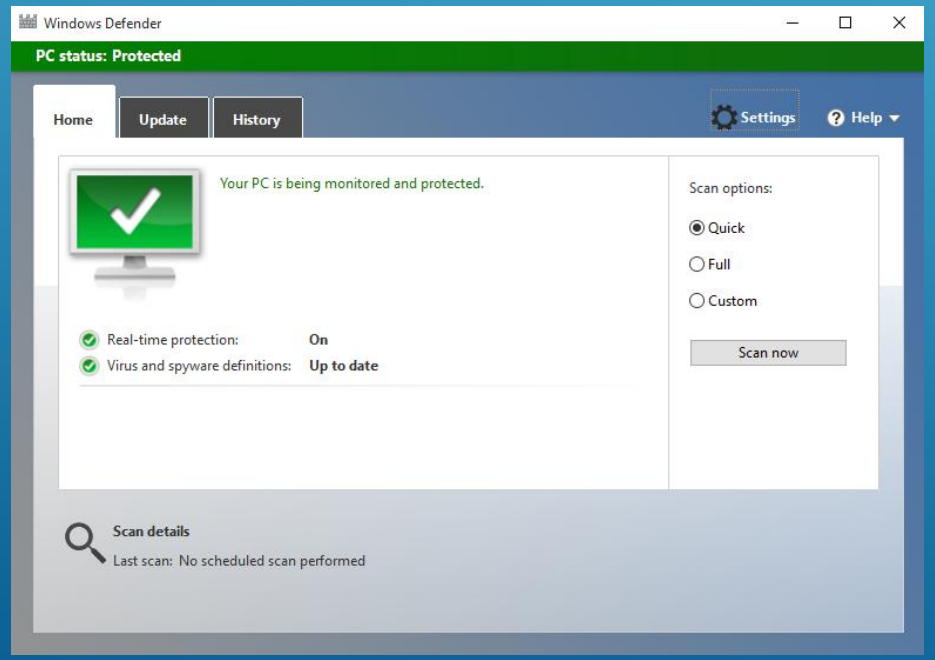
1. ANTIVIRUS / WINDOWS DEFENDER

Windows Defender หรือชื่อเก่าคือ Microsoft Security Essentials ที่ Microsoft เคยแจก Antivirus ฟรี ในสมัยยุค Windows 7 นี่เอง แต่ครั้งนี้ **Windows Defender** กลับฝังอยู่ภายในตัวระบบปฏิบัติการ Windows 8 หรือตัว Surface เองเลย ซึ่งใครใช้ Surface RT ก็หมดกังวลได้เลยว่าตัว Surface RT ไม่สามารถติดตั้งโปรแกรม Antivirus ชื่อดังได้ เพราะตัว Windows RT มันไม่ให้รันไฟล์ซอฟต์แวร์ที่ดาวน์โหลดจากเว็บไซต์ หรือซีดีต่างๆ ติดตั้งลงเครื่อง และบังคับให้โหลดผ่านทาง Windows Store อย่างเดียว แต่ Antivirus อย่าง Windows Defender นี้มันฝังอยู่ในตัวระบบปฏิบัติการ Windows 8,10 และ Windows RT แล้ว ทั้ง พีซี โน๊ตบุ๊ค แท็บเล็ตยี่ห้อต่างๆ และ Surface เองด้วย

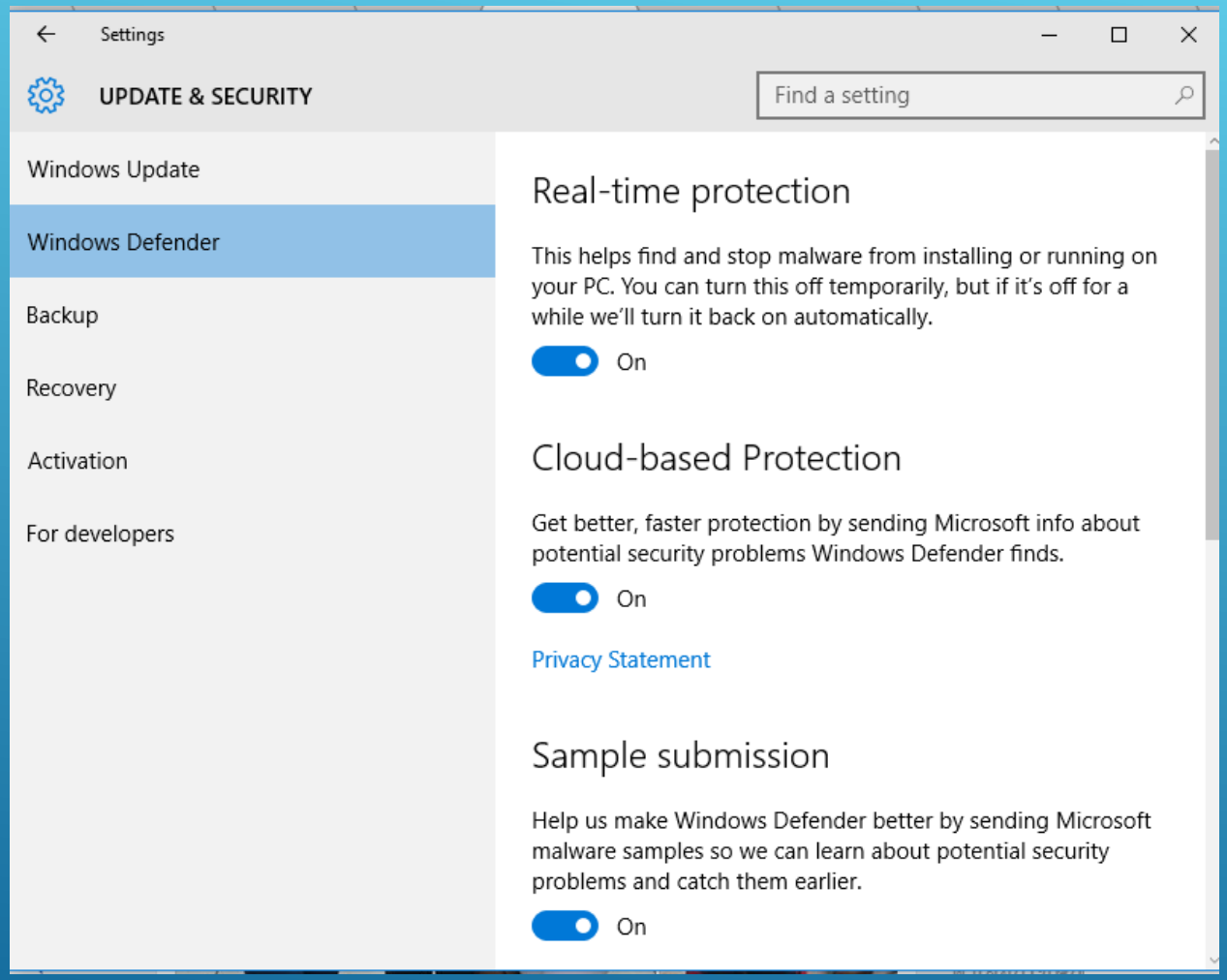


การเรียกใช้งานให้คลิกรูปแวนขยาย Search Windows แล้วพิมพ์ Control Panel แล้ว Enter





คลิกที่ windows Defender ก็จะปรากฏหน้าต่าง อ windows Defender ขึ้นมา หรือสามารถพิมพ์ windows Defender ที่ช่อง Search Windows แล้ว Enter ได้ทันที

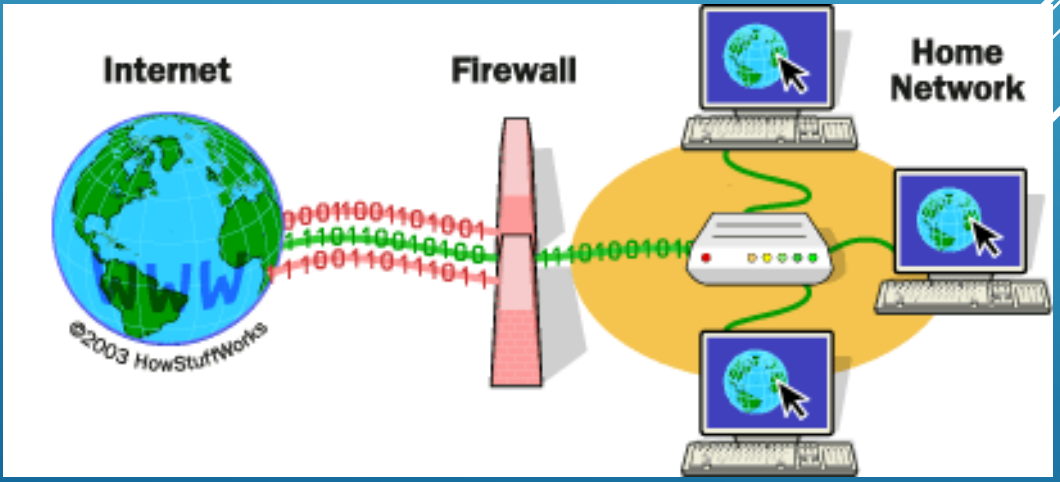


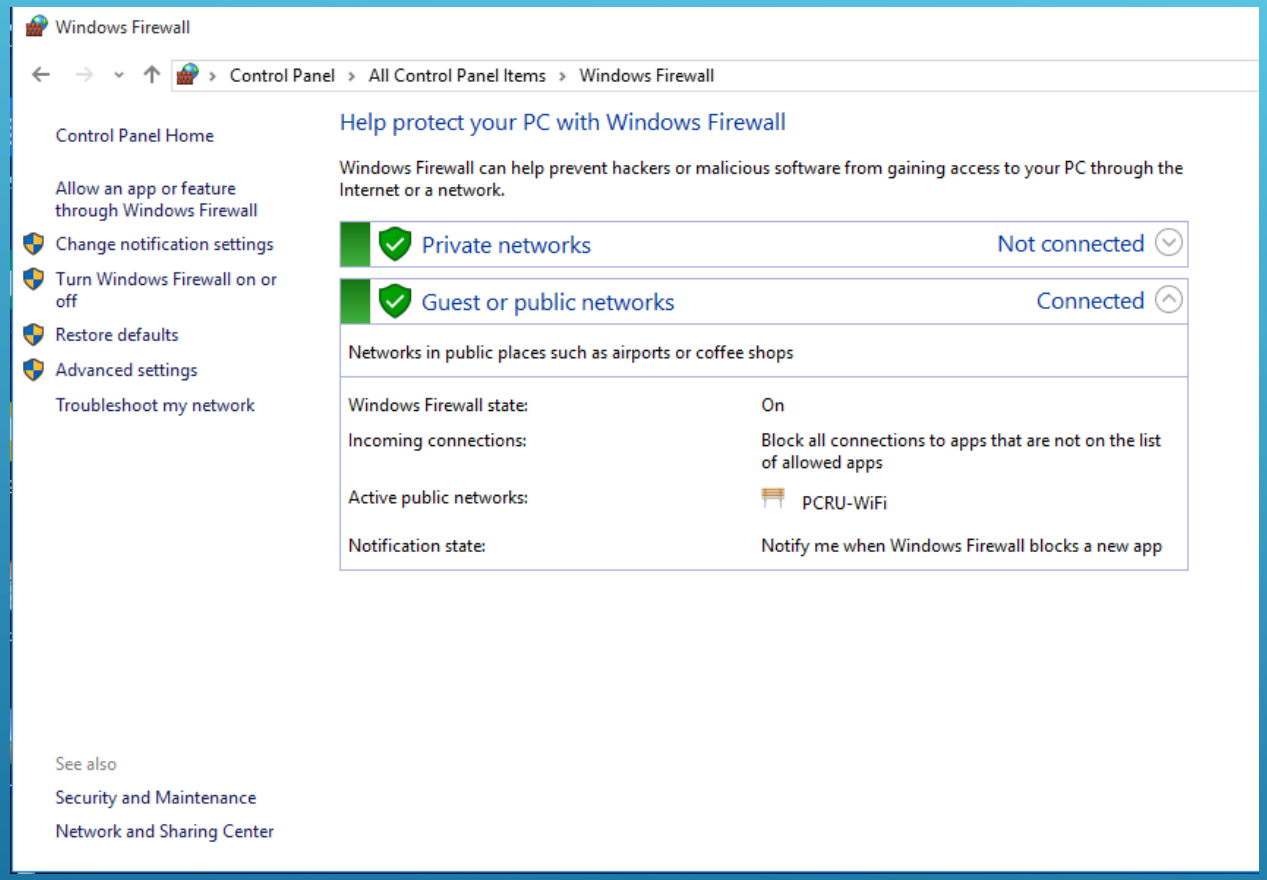
ถ้าต้องการตั้งค่า windows Defender ให้ทำการพิมพ์ windows Defender Settings Search Windows แล้ว Enter ได้ทันที

2. WINDOWS FIREWALL

Firewall คือซอฟต์แวร์หรือฮาร์ดแวร์ ทำหน้าที่ ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ตหรือเครือข่าย โดยคุณสามารถกำหนดว่าข้อมูลนั้น อนุญาตให้เพื่อนๆหรือพนักงานเข้าถึงข้อมูลไหนบ้าง หากเป็นผู้บุกรุกจะไม่มีสิทธิเข้าถึงข้อมูลนั้นได้ ทั้งนี้ การมี firewall จะตรวจสอบผู้ใช้ก่อนเข้าถึงข้อมูล

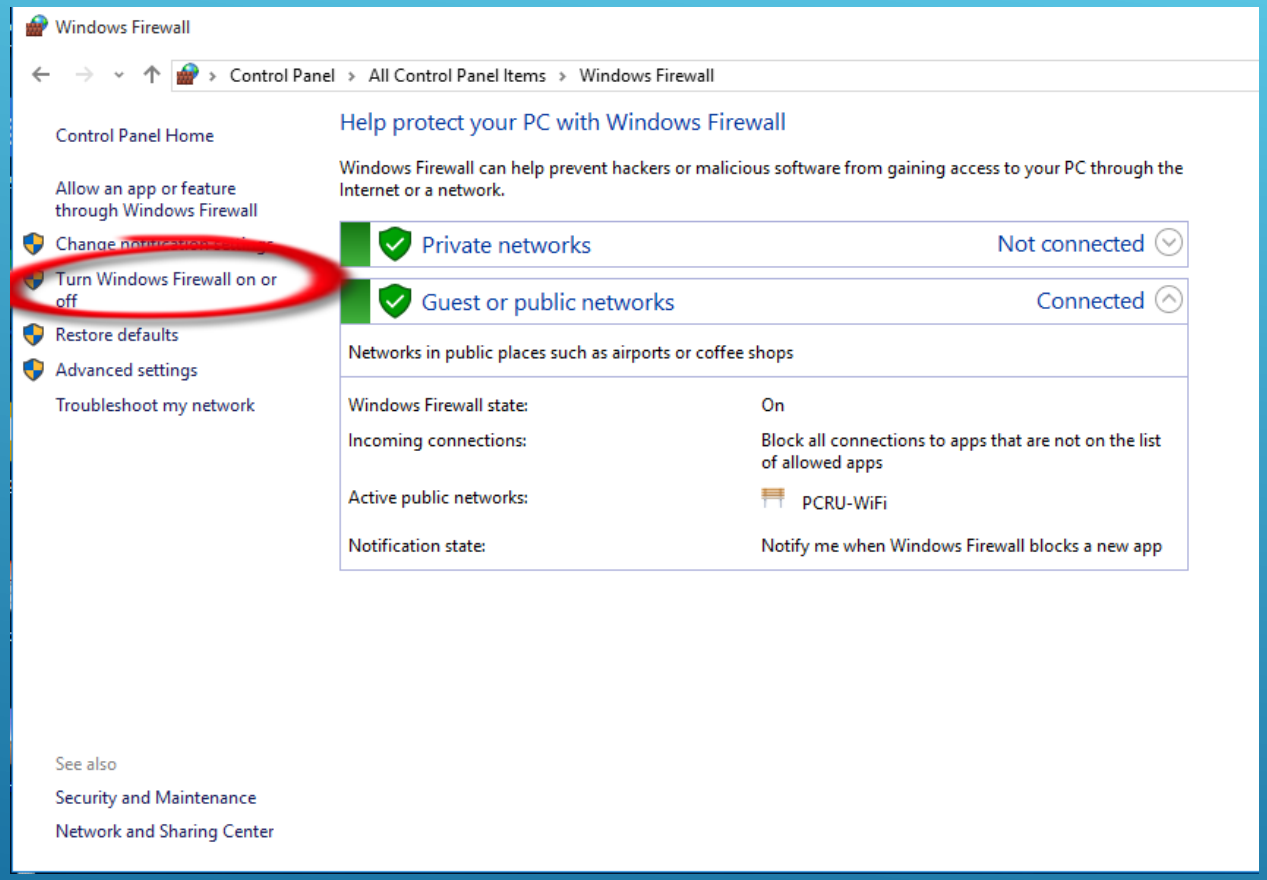
การมี Firewall นี้ จะช่วยให้คอมพิวเตอร์ในเครือข่าย ได้รับการป้องกัน ไม่ให้ Hacker หรือซอฟต์แวร์อันตราย โจมตี เข้าถึงคอมพิวเตอร์ของคุณผ่านทางเครือข่ายหรืออินเทอร์เน็ต นอกจากนี้ Firewall ยังช่วยป้องกันไม่ให้คอมพิวเตอร์ที่เป็นเหยื่อมัลแวร์นั้น ส่งซอฟต์แวร์อันตรายไปยังคอมพิวเตอร์เครื่องอื่นอีกด้วย



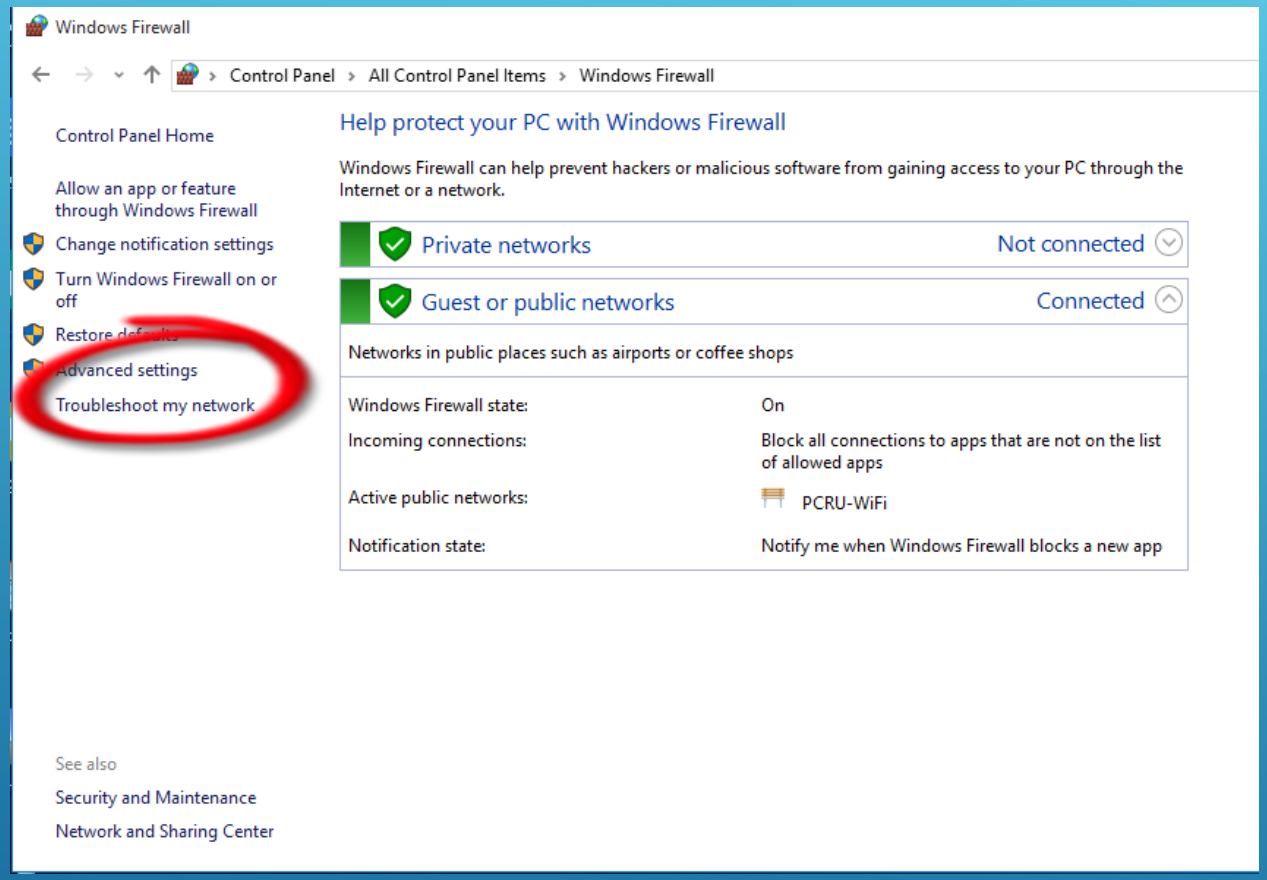


การตั้งค่า WINDOWS FIREWALL

เข้า control panel เลือก Windows Firewall ก็จะเข้าสู่หน้าต่าง Windows Firewall

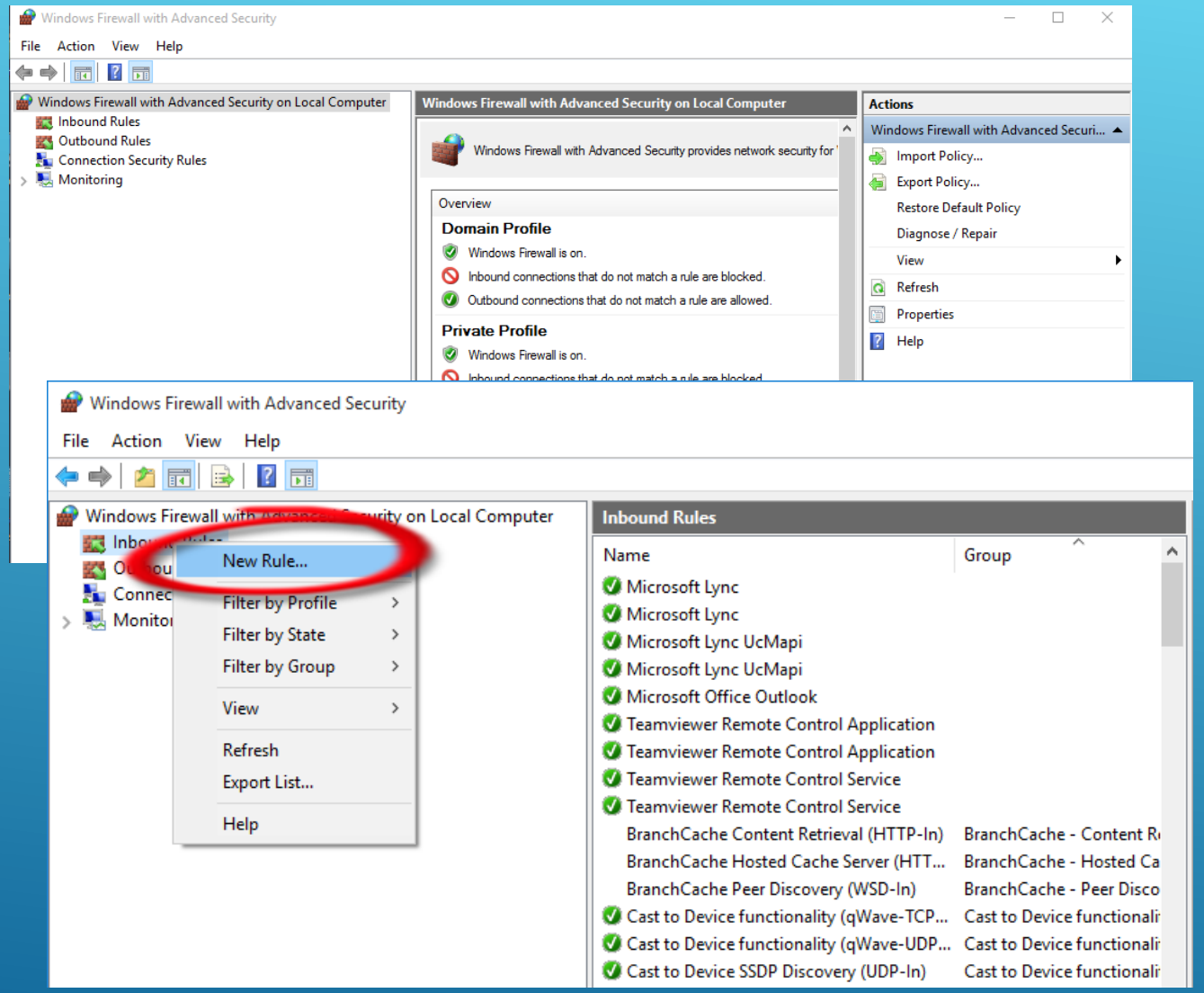


ถ้าต้องการปิดเปิด Windows Firewall ให้คลิก Turn Windows Firewall on or off ไม่แนะนำให้ปิด ควรเปิดพอร์ตที่จำเป็นเท่านั้น

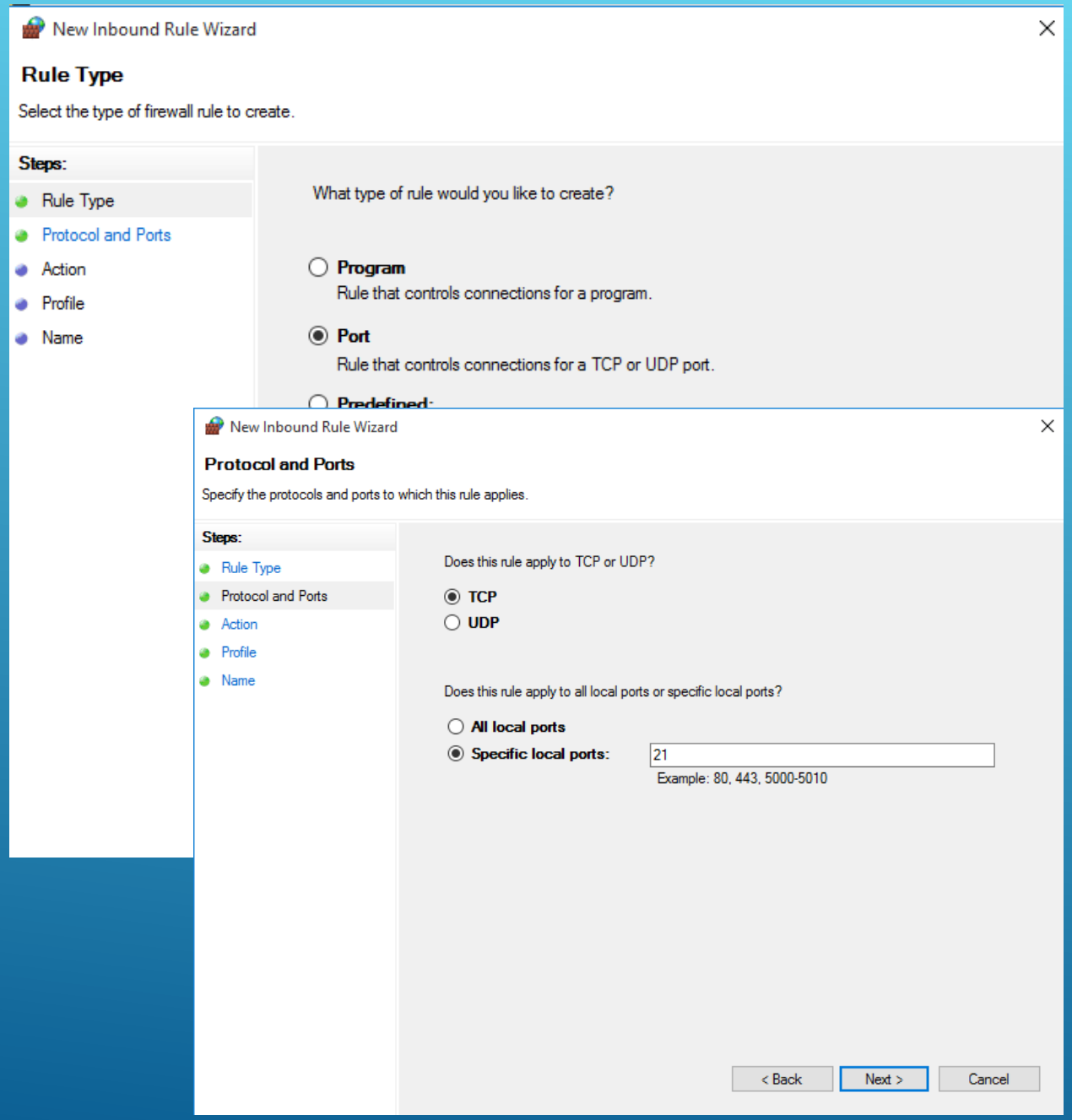


การเปิดพอร์ต WINDOWS FIREWALL

ทำการคลิก Advanced settings



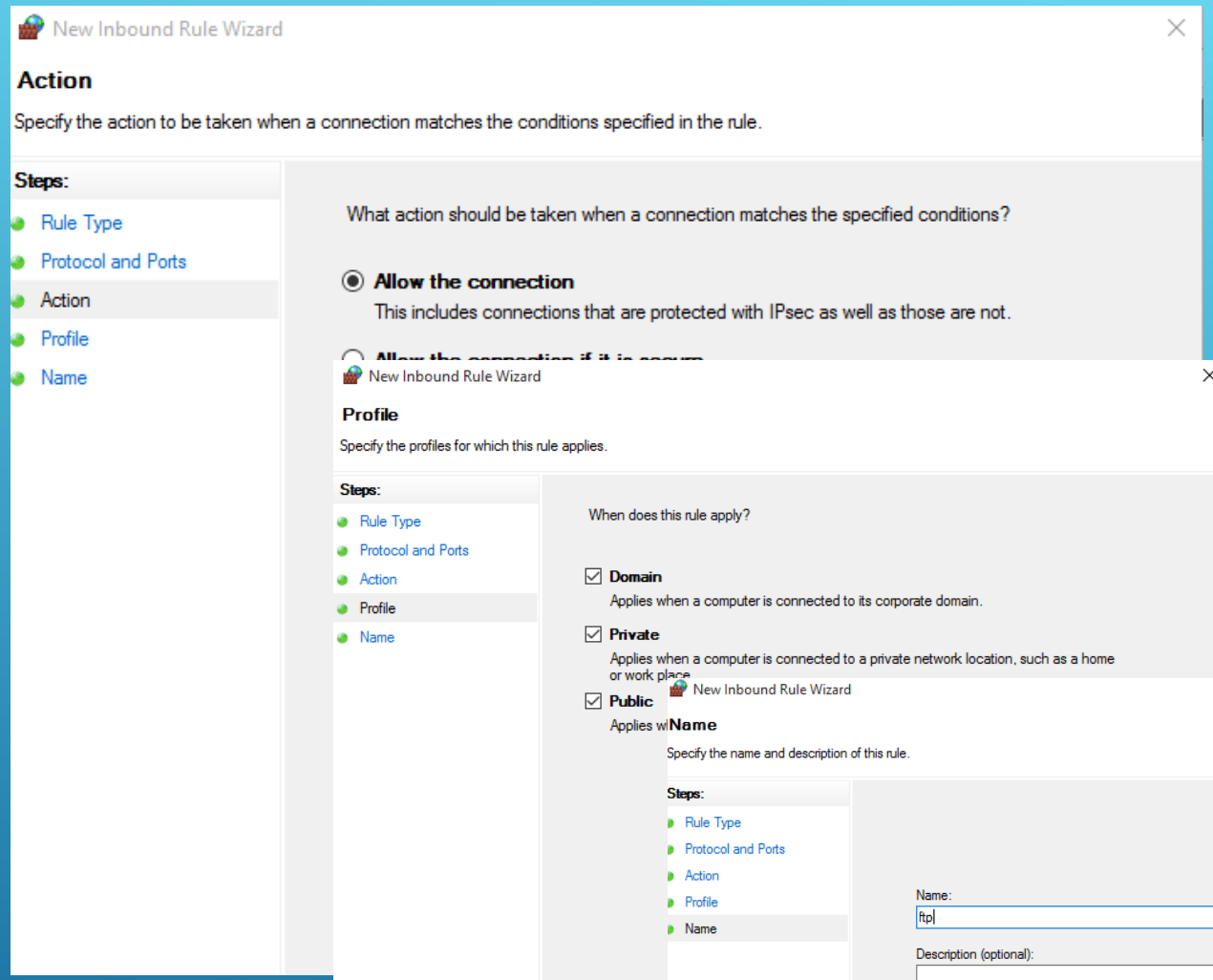
จะเข้าสู่หน้าต่าง Windows Firewall with Advanced Security ให้ทำการทคลิกที่ Inb cound Rules/ Outbound Rules แล้วเลือก New Rule...

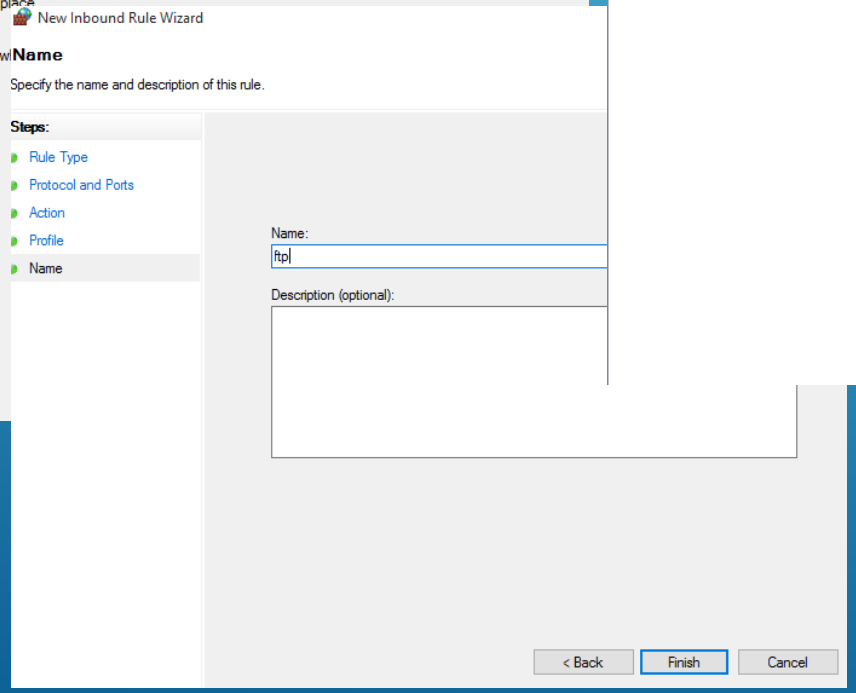


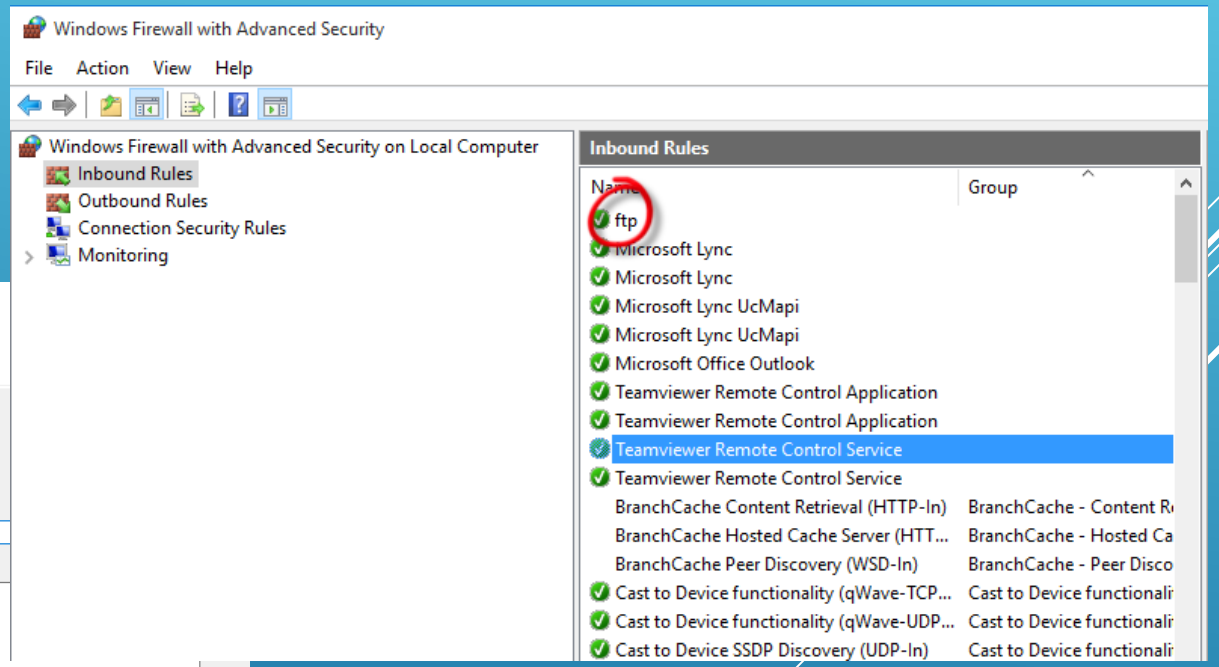
ทำการเลือกพอร์ตที่ต้องการเปิด/ปิด ถ้ารู้พอร์ตให้คลิกที่พอร์ตแล้วเลือก Next จากนั้น

https://support.apple.com/th-th/HT202944

เลือก Allow the connection คลิก Next ใส่ชื่อแล้วเลือก Finish ก็สามารถเพิ่มช่องทางติดต่อได้







3. การตั้งค่า ACCESS POINT เพื่อใช้งานในมหาวิทยาลัย

4. การค้นหาช่องสัญญาณเพื่อใช้งานให้มีประสิทธิภาพ

อาชญากรรมทางคอมพิวเตอร์ประเภทต่างๆ

ความหมายของอาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลต่าง ๆ เป็นต้น ระบบคอมพิวเตอร์ในที่นี้ หมายรวมถึงระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับระบบดังกล่าวด้วย

ประเภทของอาชญากรรมทางคอมพิวเตอร์

1. พวกมือใหม่หรือมือสมัครเล่น อยากทดลองความรู้ และส่วนใหญ่จะไม่ใช่ผู้ที่เป็นอาชญากรโดยนิสัย ไม่ได้ดำรงชีพ โดยการกระทำความผิด

2. นักเจาะข้อมูล ผู้ที่เจาะข้อมูลระบบคอมพิวเตอร์ของผู้อื่น พยายามหาความท้าทายทางเทคโนโลยี เข้าไปในเครือข่ายของผู้อื่นโดยที่ไม่ได้รับอนุญาต

3. อาชญากรในรูปแบบเดิมที่ใช้เทคโนโลยีเป็นเครื่องมือ เช่น พวกลักเล็กขโมยน้อยที่พยายามขโมยบัตรเอทีเอ็ม ของผู้อื่น

4. อาชญากรมืออาชีพ คนพวกนี้จะดำรงชีพจากการกระทำความผิด เช่น พวกที่มักจะใช้ความรู้ทางเทคโนโลยีฉ้อโกง สถาบันการเงิน หรือการจารกรรมข้อมูลไปขาย เป็นต้น

5. พวกหัวรุนแรงคลั่งอุดมการณ์หรือลัทธิ มักก่ออาชญากรรมทางคอมพิวเตอร์เพื่ออุดมการณ์ทางการเมือง เศรษฐกิจ ศาสนา หรือสิทธิมนุษยชน เป็นต้น

ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์นั้นคงจะไม่ใช่มีผลกระทบเพียงแต่ความมั่นคงของบุคคลใดบุคคลหนึ่งเพียงเท่านั้น แต่ยังมีผลกระทบไปถึงเรื่องความมั่นคงของประเทศชาติเป็นการส่วนรวม ทั้งความมั่นคงภายในและภายนอกประเทศ โดยเฉพาะในส่วนที่เกี่ยวกับข่าวกรองหรือการจารกรรมข้อมูลต่าง ๆ ที่เกี่ยวกับความมั่นคงของประเทศซึ่งในปัจจุบันได้มีการเปลี่ยนแปลงรูปแบบไปจากเดิม เช่น

1. ในปัจจุบันความมั่นคงของรัฐนั้นมิใช่จะอยู่ในวงการทหารเพียงเท่านั้น บุคคลธรรมดาก็สามารถป้องกัน หรือทำลาย ความมั่นคงของประเทศได้

2. ในปัจจุบันการป้องกันประเทศอาจไม่ได้อยู่ที่พรมแดนอีกต่อไปแล้ว แต่อยู่ที่ทำอย่างไรจึงจะไม่ให้มีการคุกคาม หรือ ทำลายโครงสร้างพื้นฐานสารสนเทศ

3. การทำจารกรรมในสมัยนี้มักจะใช้วิธีการทางเทคโนโลยีที่ซับซ้อนเกี่ยวกับเทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์บนโครงสร้างพื้นฐานสารสนเทศ ความผิดต่าง ๆ ล้วนแต่สามารถเกิดขึ้นได้ เช่น การจารกรรม การก่อการร้าย การค้ายาเสพย์ติด การแบ่งแยกดินแดน การฟอกเงิน การโจมตีระบบสาธารณูปโภคพื้นฐานของประเทศที่มีระบบคอมพิวเตอร์ควบคุม เช่น ระบบจราจร หรือระบบรถไฟฟ้า เป็นต้น ซึ่งทำให้เห็นว่า ความสัมพันธ์ระหว่างอาชญากรรมทางคอมพิวเตอร์ ความมั่นคง ของประเทศ และโครงสร้างพื้นฐานสารสนเทศของชาติ เป็นเรื่องที่ไม่สามารถแยกจากกันได้อย่างเด็ดขาด การโจมตีผ่านทางระบบโครงสร้างพื้นฐานสารสนเทศ สามารถทำได้ด้วยความเร็วเกือบเท่ากับการเคลื่อนที่ความเร็วแสง ซึ่งเหนือกว่า การเคลื่อนทัพทางบก หรือการโจมตีทางอากาศ

อาชญากรรมคอมพิวเตอร์ แบ่งเป็น 4 ลักษณะ คือ

1. การเจาะระบบรักษาความปลอดภัย ทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ

2. การเจาะเข้าไปในระบบสื่อสาร และการ รักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ

3. เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัย ของระบบปฏิบัติการ(OPERATING SYSTEM)

4. เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล โดยใช้อินเตอร์เน็ตเป็นช่องทางในการกระทำความผิด

แนวทางการแก้ไขปัญหา

ด้านตัวผู้ใช้งาน

1. การว่าจ้างอย่างรอบคอบและระมัดระวัง
2. ระวังพวกที่ไม่พอใจ
3. การแยกหน้าที่รับผิดชอบของพนักงาน
4. การจำกัดการใช้งานในระบบ
5. การป้องกันทรัพยากรข้อมูลด้วยรหัสผ่านหรือการตรวจสอบการมีสิทธิใช้งานของผู้ใช้
6. การเข้ารหัสข้อมูลโปรแกรม
7. การเฝ้าดูการเคลื่อนไหวของระบบข้อมูล
8. การตรวจสอบระบบอย่างสม่ำเสมอ
9. การให้ความรู้ผู้ร่วมงานในเรื่องระบบความปลอดภัยของข้อมูล

แนวทางการแก้ไขปัญหา

ทางภาครัฐบาล

1.ควรมีการวางแนวทางและกฎเกณฑ์ในการรวบรวมพยานหลักฐานและดำเนินคดีอาชญากรรมคอมพิวเตอร์

2.ให้มีคณะทำงานในคดีอาชญากรรมคอมพิวเตอร์ พนักงานสอบสวน

3.จัดตั้งหน่วยงานเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เพื่อให้มีเจ้าหน้าที่ที่มีความรู้ความชำนาญเฉพาะในการป้องปรามและดำเนินคดีอาชญากรรมดังกล่าว

4.บัญญัติกฎหมายเฉพาะเกี่ยวกับอาชญากรรมคอมพิวเตอร์ หรือแก้ไขเพิ่มเติมกฎหมายที่มีอยู่ให้ครอบคลุมอาชญากรรมคอมพิวเตอร์

6.เผยแพร่ความรู้เรื่องอาชญากรรมคอมพิวเตอร์แก่ผู้ใช้คอมพิวเตอร์ หน่วยงานองค์กรต่างๆ ให้เข้าใจแนวคิด วิธีการของอาชญากรทางคอมพิวเตอร์ เพื่อป้องกันตนจากอาชญากรรม